

ThinkCore W311/321/341 Linux User's Manual

Second Edition, March 2007

www.moxa.com/product



MOXA Systems Co., Ltd.

Tel: +886-2-2910-1230

Fax: +886-2-2910-1231

Web: www.moxa.com

MOXA Technical Support

Worldwide: support@moxa.com

ThinkCore W311/321/341 Linux User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2007 Moxa Systems Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of The Moxa Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of MOXA.

MOXA provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. MOXA reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, MOXA assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Table of Contents

| | | |
|------------------|---|------------|
| Chapter 1 | Introduction | 1-1 |
| | Overview..... | 1-2 |
| | Software Architecture | 1-2 |
| | Journaling Flash File System (JFFS2)..... | 1-3 |
| | Software Package | 1-4 |
| Chapter 2 | Getting Started | 2-1 |
| | Powering on the W311/321/341 | 2-2 |
| | Connecting the W311/321/341 to a PC..... | 2-2 |
| | Serial Console | 2-2 |
| | Telnet Console..... | 2-3 |
| | SSH Console | 2-4 |
| | Configuring the Ethernet Interface | 2-5 |
| | Modifying Network Settings with the Serial Console | 2-5 |
| | Modifying Network Settings over the Network | 2-6 |
| | Configuring the WLAN | 2-6 |
| | IEEE802.11a/b/g | 2-6 |
| | Using WPA_SUPPLICANT to Support WPA and WPA2..... | 2-11 |
| | SD Slot and USB for Storage Expansion | 2-11 |
| | Test Program—Developing Hello.c | 2-13 |
| | Installing the Tool Chain (Linux)..... | 2-13 |
| | Checking the Flash Memory Space | 2-13 |
| | Compiling Hello.c | 2-14 |
| | Uploading and Running the “Hello” Program..... | 2-15 |
| | Developing Your First Application | 2-15 |
| | Testing Environment | 2-16 |
| | Compiling tcps2.c..... | 2-17 |
| | Uploading and Running the “tcps2-release” Program | 2-18 |
| | Testing Procedure Summary | 2-20 |
| Chapter 3 | Managing Embedded Linux | 3-1 |
| | System Version Information..... | 3-2 |
| | System Image Backup..... | 3-2 |
| | Upgrading the Firmware..... | 3-2 |
| | Loading Factory Defaults | 3-5 |
| | Backing Up the User Directory | 3-5 |
| | Deploying the User Directory to Additional W311/321/341 Units | 3-6 |
| | Enabling and Disabling Daemons..... | 3-6 |
| | Setting the Run-Level | 3-8 |
| | Adjusting the System Time | 3-9 |
| | Setting the Time Manually | 3-9 |
| | NTP Client..... | 3-10 |
| | Updating the Time Automatically..... | 3-10 |
| | Cron—Daemon to Execute Scheduled Commands | 3-11 |

| | | |
|------------------|---|------------|
| Chapter 4 | Managing Communications | 4-1 |
| | Telnet / FTP | 4-2 |
| | DNS | 4-2 |
| | Web Service—Apache | 4-2 |
| | Installing PHP for Apache Web Server | 4-4 |
| | IPTABLES | 4-7 |
| | NAT..... | 4-11 |
| | NAT Example | 4-11 |
| | Enabling NAT at Bootup | 4-12 |
| | Dial-up Service—PPP..... | 4-12 |
| | PPPoE | 4-15 |
| | NFS (Network File System)..... | 4-17 |
| | Setting up the W311/321/341 as an NFS Client | 4-18 |
| | Mail..... | 4-18 |
| | SNMP | 4-18 |
| | OpenVPN..... | 4-27 |
| Chapter 5 | Tool Chains for Application Development..... | 5-1 |
| | Linux Tool Chain | 5-2 |
| | Steps for Installing the Linux Tool Chain..... | 5-2 |
| | Compilation for Applications | 5-2 |
| | On-Line Debugging with GDB | 5-3 |
| | Windows Tool Chain..... | 5-4 |
| | System Requirements for Windows Tool Chain..... | 5-4 |
| | Steps for Installing Windows Tool Chain..... | 5-4 |
| | Using the BASH Shell..... | 5-9 |
| | Compilation for Applications | 5-10 |
| | On-Line Debugging with Insight..... | 5-12 |
| Chapter 6 | Programmer's Guide..... | 6-1 |
| | Flash Memory Map..... | 6-2 |
| | Device API..... | 6-2 |
| | RTC (Real Time Clock) | 6-2 |
| | Buzzer | 6-3 |
| | WDT (Watch Dog Timer) | 6-3 |
| | UART..... | 6-7 |
| | DO | 6-8 |
| Chapter 7 | Software Lock..... | 7-1 |
| Chapter 8 | UC Finder | 8-1 |
| | Windows UC Finder | 8-2 |
| | Installing the Software..... | 8-2 |
| | Broadcast Search | 8-3 |
| | Linux ucfinder..... | 8-4 |

| | | |
|-------------------|---|------------|
| Appendix A | System Commands..... | A-1 |
| | busybox (V0.60.4): Linux normal command utility collection..... | A-1 |
| | File manager..... | A-1 |
| | Editor..... | A-1 |
| | Network..... | A-1 |
| | Process..... | A-2 |
| | Other..... | A-2 |
| | MOXA special utilities..... | A-2 |
| Appendix B | Service Information..... | B-1 |
| | MOXA Internet Services..... | B-2 |
| | Problem Report Form | B-3 |
| | Product Return Procedure | B-4 |

The MOXA ThinkCore W311/321/341 are RISC-based ready-to-run wireless embedded computers with 802.11a/b/g WLAN, one 10/100 Mbps Ethernet port, an internal SD socket, 1/2/4 RS-232/422/485 serial ports, two USB 2.0 hosts, one relay output channel, and pre-installed Linux operating system. The W311/321/341 offer high performance communication and unlimited storage in a super compact, palm-size ARM9 box. The ThinkCore W300 Series is the right solution for embedded applications that are used in hard-to-wire environments and that require a large amount of memory, but that must be housed in a small space without sacrificing performance.

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Software Architecture**
 - Journaling Flash File System (JFFS2)
 - Software Package

Overview

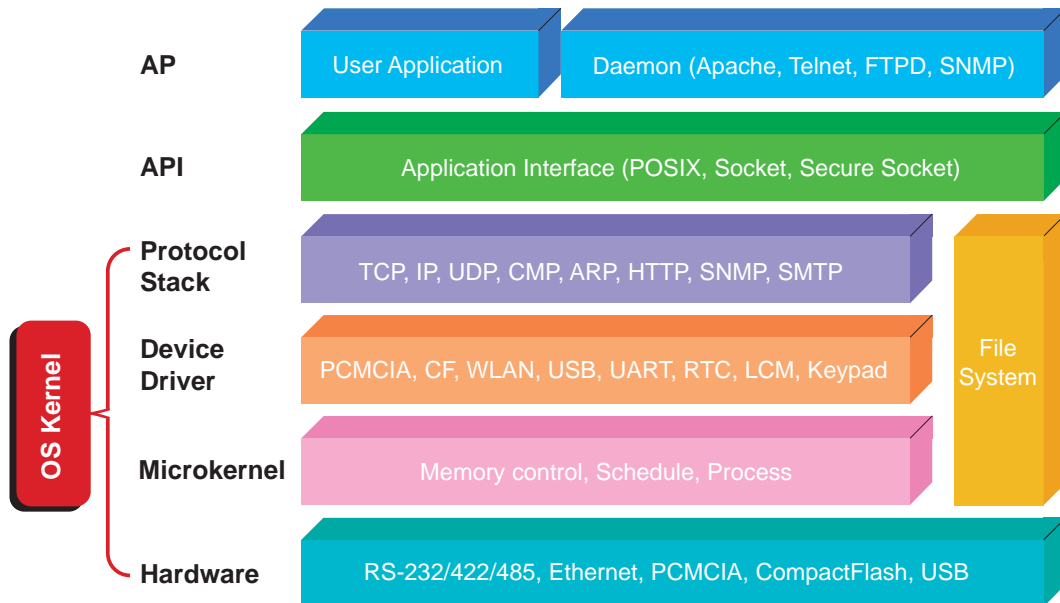
The ThinkCore W311/321/341 wireless embedded computers support 802.11a/b/g wireless LANs with data encryption functions, including the common WEP and powerful WPA and WPA2, to establish a secure transmission tunnel over a WLAN.

ThinkCore W300 Series Embedded Computers use a MOXA ART 192 Mhz RISC CPU. Unlike the X86 CPU, which uses a CISC design, the RISC architecture and modern semiconductor technology provide these embedded computers with a powerful computing engine and communication functions, but without generating a lot of heat. A 16 MB NOR Flash ROM and on-board SDRAM (64 MB for W341 and 32 MB for W311/321) give you enough memory to install your application software directly on the embedded computer. In addition, dual LAN ports are built right into the RISC CPU. This network capability, in combination with the ability to control serial devices, makes the ThinkCore W300 Series ideal as communication platforms for data acquisition and industrial control applications.

The pre-installed Linux operating system (OS) provides an open software operating system for your software program development. Software written for desktop PCs can be easily ported to the computer with a GNU cross compiler, without needing to modify the source code. The OS, device drivers (e.g., serial and buzzer control), and your own applications, can all be stored in the NOR Flash memory.

Software Architecture

The Linux operating system that is pre-installed in the W311/321/341 follows the standard Linux architecture, making it easy to accept programs that follow the POSIX standard. Program porting is done with the GNU Tool Chain provided by MOXA. In addition to Standard POSIX APIs, device drivers for the USB storage, buzzer and Network controls, and UART are also included in the Linux OS.



The W311/321/341's built-in Flash ROM is partitioned into **Boot Loader**, **Linux Kernel**, **Root File System**, and **User directory** partitions.

In order to prevent user applications from crashing the Root File System, the W311/321/341 use a specially designed **Root File System with Protected Configuration** for emergency use. This **Root File System** comes with serial and Ethernet communication capability for users to load the

Factory Default Image file. The user directory saves the user's settings and application.

To improve system reliability, the W311/321/341 have a built-in mechanism that prevents the system from crashing. When the Linux kernel boots up, the kernel will mount the root file system for read only, and then enable services and daemons. At the same time, the kernel will start searching for system configuration parameters via *rc* or *inittab*.

Normally, the kernel uses the Root File System to boot up the system. The Root File System is protected, and cannot be changed by the user. This type of setup creates a "safe" zone.

For more information about the memory map and programming, refer to Chapter 6, *Programmer's Guide*.

Journaling Flash File System (JFFS2)

The Root File System and User directory in the flash memory is formatted with the **Journaling Flash File System (JFFS2)**. The formatting process places a compressed file system in the flash memory. This operation is transparent to the user.

The Journaling Flash File System (JFFS2), which was developed by Axis Communications in Sweden, puts a file system directly on the flash, instead of emulating a block device. It is designed for use on flash-ROM chips and recognizes the special write requirements of a flash-ROM chip. JFFS2 implements wear-leveling to extend the life of the flash disk, and stores the flash directory structure in the RAM. A log-structured file system is maintained at all times. The system is always consistent, even if it encounters crashes or improper power-downs, and does not require *fsck* (file system check) on boot-up.

JFFS2 is the newest version of JFFS. It provides improved wear-leveling and garbage-collection performance, improved RAM footprint and response to system-memory pressure, improved concurrency and support for suspending flash erases, marking of bad sectors with continued use of the remaining good sectors (enhancing the write-life of the devices), native data compression inside the file system design, and support for hard links.

The key features of JFFS2 are:

- Targets the Flash ROM Directly
- Robustness
- Consistency across power failures
- No integrity scan (fsck) is required at boot time after normal or abnormal shutdown
- Explicit wear leveling
- Transparent compression

Although JFFS2 is a journaling file system, this does not preclude the loss of data. The file system will remain in a consistent state across power failures and will always be mountable. However, if the board is powered down during a write then the incomplete write will be rolled back on the next boot, but writes that have already been completed will not be affected.

Additional information about JFFS2 is available at:

<http://sources.redhat.com/jffs2/jffs2.pdf>

<http://developer.axis.com/software/jffs/>

<http://www.linux-mtd.infradead.org/>

Software Package

| | |
|---------------------------|--|
| Boot Loader | Moxa Boot Loader (v1.2) |
| Kernel | Linux 2.6.9 |
| Protocol Stack | ARP, PPP, CHAP, PAP, IPv4, ICMP, TCP, UDP, DHCP, FTP, SNMP V1/V3, HTTP, NTP, NFS, SMTP, SSH 1.0/2.0, SSL, Telnet, PPPoE, OpenVPN |
| File System | JFFS2, NFS, Ext2, Ext3, VFAT/FAT |
| OS shell command | Bash |
| Busybox | Linux normal command utility collection |
| Utilities | |
| tinylogin | login and user manager utility |
| telnet | telnet client program |
| ftp | FTP client program |
| smtpclient | email utility |
| scp | Secure file transfer Client Program |
| Daemons | |
| pppd | dial in/out over serial port daemon |
| snmpd | snmpd agent daemon |
| telnetd | telnet server daemon |
| inetd | TCP server manager program |
| ftpd | ftp server daemon |
| apache | web server daemon |
| sshd | secure shell server |
| openvpn | virtual private network |
| openssl | open SSL |
| Linux Tool Chain | |
| Gcc (V3.3.2) | C/C++ PC Cross Compiler |
| GDB (V5.3) | Source Level Debug Server |
| Glibc (V2.2.5) | POSIX standard C library |
| Windows Tool Chain | |
| Gcc (V3.3.2) | C/C++ PC Cross Compiler |
| Glibc(V2.2.5) | POSIX standard C library |
| Insight (V6.1) | Windows environment source level debug utility |

2

Getting Started

In this chapter, we explain how to connect the W311/321/341, how to turn on the power, how to get started programming, and how to use the W311/321/341's other functions.

The following topics are covered in this chapter:

- ❑ **Powering on the W311/321/341**
- ❑ **Connecting the W311/321/341 to a PC**
 - Serial Console
 - Telnet Console
 - SSH Console
- ❑ **Configuring the Ethernet Interface**
 - Modifying Network Settings with the Serial Console
 - Modifying Network Settings over the Network
- ❑ **Configuring the WLAN**
 - IEEE802.11a/b/g
- ❑ **Using WPA_SUPPLICANT to Support WPA and WPA2**
- ❑ **SD Socket and USB for Storage Expansion**
- ❑ **Test Program—Developing Hello.c**
 - Installing the Tool Chain (Linux)
 - Checking the Flash Memory Space
 - Compiling Hello.c
 - Uploading and Running the “Hello” Program
- ❑ **Developing Your First Application**
 - Testing Environment
 - Compiling tcps2.c
 - Uploading and Running the “tcps2-release” Program
 - Testing Procedure Summary

Powering on the W311/321/341

Connect the SG wire to the shielded contact located in the upper left corner of the W311/321/341, and then power on the computer by connecting it to the power adaptor. It takes about 30 to 60 seconds for the system to boot up. Once the system is ready, the Ready LED will light up.

NOTE After connecting the W311/321/341 to the power supply, it will take about 30 to 60 seconds for the operating system to boot up. The green Ready LED will not turn on until the operating system is ready.



ATTENTION

This product is intended to be supplied by a Listed Power Unit with output marked "LPS" and rated for 12-48 VDC, 600 mA (minimum requirements).

Connecting the W311/321/341 to a PC

There are two ways to connect the W311/321/341 to a PC: through the serial console and by Telnet over the network.

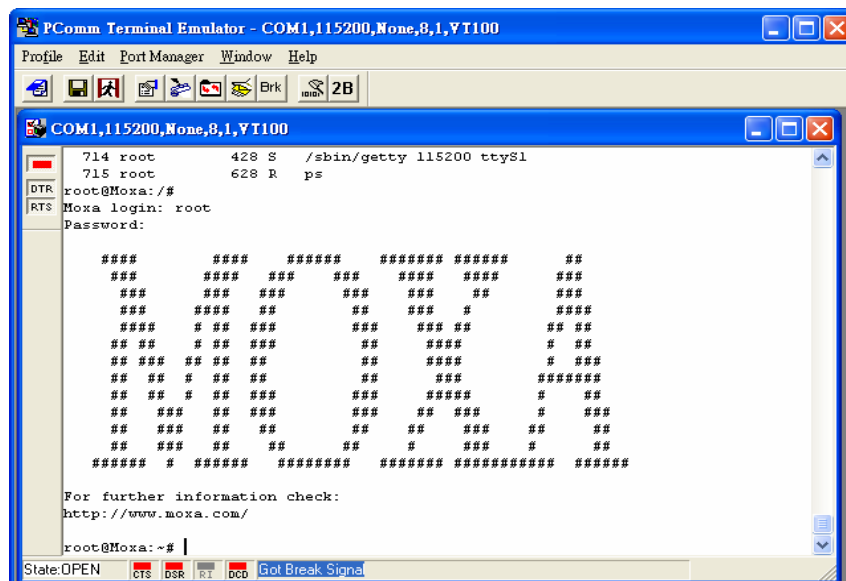
Serial Console

The serial console gives users a convenient way of connecting to the W311/321/341. This method is particularly useful when using the computer for the first time. The serial console is useful for connecting the W311/321/341 when you do not know either of the two IP addresses.

Use the serial console port settings shown below.

| | |
|---------------------|------------|
| Baudrate | 115200 bps |
| Parity | None |
| Data bits | 8 |
| Stop bits: | 1 |
| Flow Control | None |
| Terminal | VT100 |

The following window will open when a connection has been established.



To log in, type the Login name and password as requested. The default values are both **root**:

Login: root
Password: root

Telnet Console

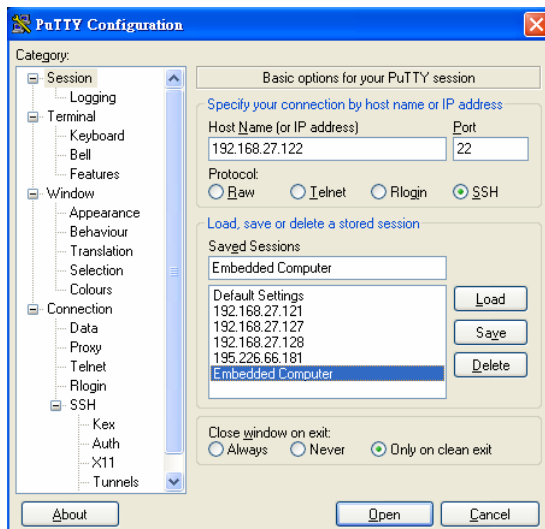
If you know at least one of the two IP addresses and netmasks, then you can use Telnet to connect to the W311/321/341's console utility. The default IP address and Netmask for each of the two ports are given below:

| | Default IP Address | Netmask |
|---------------------|--------------------|---------------|
| LAN 1 | 192.168.3.127 | 255.255.255.0 |
| WIRELESS LAN | 192.168.4.127 | 255.255.255.0 |

Use a cross-over Ethernet cable to connect directly from your PC to the W311/321/341. You should first modify your PC's IP address and netmask so that your PC is on the same subnet as one of W311/321/341's two LAN ports. For example, if you connect to LAN 1, you can set your PC's IP address to 192.168.3.126 and netmask to 255.255.255.0. If you connect to the WIRELESS LAN, you can set your PC's IP address to 192.168.4.126 and netmask to 255.255.255.0 using a wireless AP router.

Use a straight-through Ethernet cable to connect to a hub or switch that is connected to your local LAN. The default IP addresses and netmasks are shown above. To log in, type the Login name and password as requested. The default values are both **root**:

Login: root
Password: root



Linux Users

From a Linux machine, use the “ssh” command to access the W311/321/341’s console utility via SSH.

```
#ssh 192.168.3.127
```

Select **yes** to complete the connection.

```
[root@bee_notebook root]# ssh 192.168.3.127
The authenticity of host '192.168.3.127 (192.168.3.127)' can't be established.
RSA key fingerprint is 8b:ee:ef:84:41:25:fc:cd:2a:f2:92:8f:cb:1f:6b:2f.
Are you sure you want to continue connection (yes/no)? yes_
```

NOTE SSH provides better security compared to Telnet for accessing the W311/321/341’s console utility over the network.

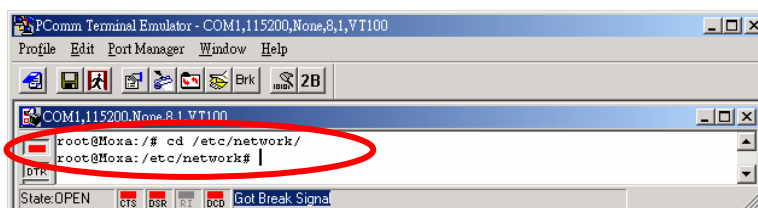
Configuring the Ethernet Interface

The network settings of the W311/321/341 can be modified with the serial console port, or online over the network.

Modifying Network Settings with the Serial Console

In this section, we use the serial console to configure the network settings of the target computer.

1. Follow the instructions given in a previous section to access the Console Utility of the target computer via the serial console port, and then type `#cd /etc/network` to change directories.



2. Type `#vi interfaces` to edit the network configuration file with vi editor. You can configure the Ethernet ports of the W341 for **static** or **dynamic** (DHCP) IP addresses.

Static IP addresses

As shown in the table below, 4 network addresses must be modified: **address**, **network**, **netmask**, and **broadcast**. The default IP address for LAN1 is 192.168.3.127, with default netmask of 255.255.255.0.

Dynamic IP addresses

By default, the W311/321/341 are configured for “static” IP addresses. To configure one or both LAN ports to request an IP address dynamically, replace **static** with **dhcp** and then delete the address, network, netmask, and broadcast lines.

| Default Setting for LAN1 | Dynamic Setting using DHCP |
|---|--|
| <pre>iface eth0 inet static address 192.168.3.127 network: 192.168.3.0 netmask 255.255.255.0 broadcast 192.168.3.255</pre> | <pre>iface eth0 inet dhcp</pre> |

3. After the boot settings of the LAN interface have been modified, issue the following command to activate the LAN settings immediately:

```
#/etc/init.d/networking restart
```

NOTE After changing the IP settings, use the **networking restart** command to activate the new IP address.

Modifying Network Settings over the Network

IP settings can be activated over the network, but the new settings will not be saved to the flash ROM without modifying the file `/etc/network/interfaces`.

For example, type the command `#ifconfig eth0 192.168.1.1` to change the IP address of LAN1 to 192.168.1.1.

```
root@Moxa:~# ifconfig eth0 192.168.27.125
root@Moxa:~# _
```

Configuring the WLAN

IEEE802.11a/b/g

Use one of the following options to configure the WLAN for IEEE802.11a/b/g:

1. **Using the config file to set up your wireless system**

The config file is `/etc/wireless.conf`. The config file is read by the OS when the W311/321/341 unit boots up. You may also use the `load_wlan` command to force your wireless to run the config file and set up your wireless LAN card after the W311/321/341 unit is already up and running. The `/etc/wireless.conf` file format is shown below:

Default Setting for WIRELESS LAN

```
iface eth1 inet static
address 192.168.4.127
network: 192.168.4.0
netmask 255.255.255.0
broadcast 192.168.4.255
```

Dynamic Setting using DHCP

```
iface eth1 inet dhcp
```

After the boot settings of the LAN interface have been modified, issue the following command to activate the LAN settings immediately:

```
#/etc/init.d/networking restart
```

3. Using iwconfig / iwpriv Utility to set up the wireless configuration

Using iwpriv eth1 essid ESSIDNAME

iwconfig eth1 essid ESSIDNAME → set up wireless essid
 iwconfig eth1 key KEYVALUE open → set up wireless wep key
 iwconfig eth1 mode infra → set up wireless mode

CountryRegion—Sets the channels for your particular country / region

Using iwpriv eth1 set_Region REGION

| REGION | Explanation |
|-------------------|-------------------------------|
| 1 (USA) (default) | Use 802.11g channels 1 to 11 |
| 2 (Taiwan/Europe) | Use 802.11g channels 1 to 13 |
| 3 (France) | Use 802.11g channels 10 to 13 |
| 4 (Japan) | Use 802.11g channels 1 to 14 |
| 5 (Israel) | Use 802.11g channels 3 to 9 |
| 6 (Mexico) | Use 802.11g channels 10 , 11 |

WirelessMode—Sets the wireless mode

Using iwpriv eth1 set_mac_mode **Setting**

Note: infrastruct just support mixed/a mode; Ad-hoc support b/g/a mode

| Setting | Explanation |
|-------------|----------------|
| 1 (default) | 11a/mixed(b.g) |
| 2 | 11g only |
| 3 | 11b only |
| 4 | 11a only |

SSID—Sets the softAP SSID

Using iwconfig eth1 essid **Setting**

| Setting |
|--------------------|
| Any 32-byte string |

NetworkType—Sets the wireless operation mode

Using iwconfig eth1 mode **Setting**

| Setting | Explanation |
|---------|---|
| managed | Infrastructure mode (uses access points to transmit data) |
| ad-hoc | Adhoc mode (transmits data from host to host) |

Channel—Sets the channel

Using iwconfig eth1 channel **Setting**

Note: Infrastruct couldn't set channel

Freq—Sets the channel frequency

Using iwconfig eth1 freq **Setting(G,M,K)**

Note: Infrastruct couldn't set freq

802.11b,g Channel and Frequency Table

| Channel | Frequence |
|---------|-----------|
| 1 | 2412(K) |
| 2 | 2417(K) |
| 3 | 2422(K) |
| 4 | 2427(K) |
| 5 | 2432(K) |
| 6 | 2437(K) |
| 7 | 2442(K) |
| 8 | 2447(K) |
| 9 | 2452(K) |
| 10 | 2457(K) |
| 11 | 2462(K) |
| 12 | 2467(K) |
| 13 | 2472(K) |
| 14 | 2484(K) |

802.11a Channel and Frequency Table

| Channel | Frequence |
|---------|-----------|
| 36 | 5180 (K) |
| 40 | 5200 (K) |
| 44 | 5220 (K) |
| 48 | 5240 (K) |
| 52 | 5260 (K) |
| 56 | 5280 (K) |
| 60 | 5300 (K) |
| 64 | 5320 (K) |
| 100 | 5500 (K) |
| 104 | 5520 (K) |
| 108 | 5540 (K) |
| 112 | 5560 (K) |
| 116 | 5580 (K) |
| 120 | 5600 (K) |
| 124 | 5620(K) |
| 128 | 5640 (K) |
| 132 | 5660 (K) |
| 136 | 5680 (K) |

| | |
|-----|----------|
| 140 | 5700 (K) |
| 184 | 4920 (K) |
| 188 | 4940 (K) |
| 192 | 4960(K) |
| 196 | 4980 (K) |
| 8 | 5040 (K) |
| 12 | 5060 (K) |
| 16 | 5080 (K) |
| 34 | 5170 (K) |
| 38 | 5190 (K) |
| 42 | 5210 (K) |
| 46 | 5230 (K) |
| 149 | 5745 (K) |
| 153 | 5765 (K) |
| 157 | 5785 (K) |
| 161 | 5805 (K) |
| 165 | 5825 (K) |

AuthMode—Sets the authentication mode

Using iwpriv eth1 set_auth **Setting**

| Setting | Explanation |
|---------|---------------|
| 0 | OPEN |
| 1 | SHARED |
| 2 | AUTO(default) |

KeyStr—Sets Key Support string key and hex key

EncryptType—Just Support **NONE** , **WEP64** and **WEP128** depend on your key length

Using iwpriv eth1 key s:KEYVALUE (open) → support string key

Using iwpriv eth1 key KEYVALUE (open) → support hex key

RTSThreshold—Sets the RTS threshold

Using iwpriv eth1 rts **Setting**

| Setting |
|-----------|
| 1 to 2347 |

FragThreshold—Sets the fragment threshold

Using iwpriv eth1 frag **Setting**

| Setting |
|-------------|
| 256 to 2346 |

Moxa Repeat—Sets the Repeat function through adhoc method

Using iwpriv eth1 set_moxa_repeat

Using WPA_SUPPLICANT to Support WPA and WPA2

This embedded computer supports the WPA and WPA2 functions using the `/bin/wpa_supplicant` program. We wrote a shell script to help you use this function:

Step 1:

Edit the `ssid` and `psk` variables in the file `etc/wpa_supplicant.conf`.

```
network={
  ssid="12345678901"
  key_mgmt=WPA-PSK
  proto=WPA RSN
  pairwise=TKIP CCMP
  group=TKIP CCMP
  psk="0987654321234"
}
```

Step 2:

Type `/etc/init.d/wpa.sh eth1 start` to enable this function. To stop the function, type `/etc/init.d/wpa.sh eth1 stop`

SD Slot and USB for Storage Expansion

The W341 and W321 provide an SD slot for storage expansion. MOXA provides an SD flash disk for plug & play expansion that allows users to plug in a Secure Digital (SD) memory card compliant with the SD standard V1.0 for up to 1 GB of additional memory space. The following steps show you how to install SD card into the W341 and W321.

W321

The SD slot is located on the right side of the W321 enclosure. To install an SD card, you must first remove the SD slot's protective cover to access the slot, and then plug the SD card directly into the slot.

The SD card will be mounted at `/mnt/sd`. Detailed installation instructions are shown below:

Step 1: Use a screwdriver to remove the screws holding the SD slot's outer cover.



Step 2: After removing the cover, insert the SD memory card as shown.



W341

The SD slot is located on the front panel of the W341. To install an SD card, you must first remove the SD slot's protective cover to access the slot, and then plug the SD card directly into the slot.

The SD card will be mounted at `/mnt/sd`. Detailed installation instructions are shown below:

Step 1: Use a screwdriver to remove the screws holding the SD slot's outer cover, and then remove the cover.



Step 2: Insert the SD memory card as shown.



NOTE: To remove the SD card from the slot, press the SD card in slightly with your finger, and then remove your finger to cause the card to spring out partially. You may now grasp the top of the card with two fingers and pull it out.

Before removing the SD card, remember to type `/sync` to ensure that your data has been written.

In addition to the SD socket, two USB 2.0 ports are located on the W341's upper panel. The USB host is also designed for storage expansion. To use a USB flash disk to expand the storage space, plug the USB flash disk into the USB port. The flash disk will be detected automatically, and its file partition will be mounted into the OS. The USB storage will be mounted in one of four directories: `/mnt/usbstorage1`, `/mnt/usbstorage2`, `/mnt/usbstorage3`, or `/mnt/usbstorage4`.

Test Program—Developing Hello.c

In this section, we use the standard “Hello” programming example to illustrate how to develop a program for the W311/321/341. In general, program development involves the following seven steps.

Step 1:

Connect the W311/321/341 to a Linux PC.

Step 2:

Install Tool Chain (GNU Cross Compiler & glibc).

Step 3:

Set the cross compiler and glibc environment variables.

Step 4:

Code and compile the program.

Step 5:

Download the program to the W311/321/341 using FTP or NFS.

Step 6:

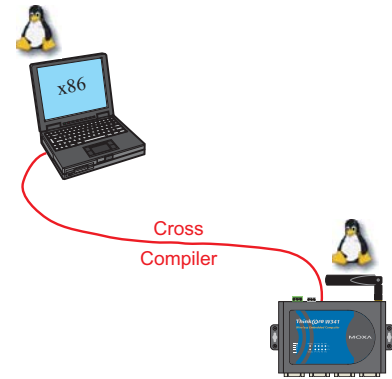
Debug the program

→ If bugs are found, return to Step 4.

→ If no bugs are found, continue with Step 7.

Step 7:

Back up the user directory (distribute the program to additional W311/321/341 units if needed).



Installing the Tool Chain (Linux)

The Linux Operating System must be pre-installed in the PC before installing the W311/321/341 GNU Tool Chain. Fedora core or compatible versions are recommended. The Tool Chain requires approximately 100 MB of hard disk space on your PC. The W311/321/341 Tool Chain software is located on the W311/321/341 CD. To install the Tool Chain, insert the CD into your PC and then issue the following commands:

```
#mount /dev/cdrom /mnt/cdrom
#sh /mnt/cdrom/tool-chain/linux/install.sh
```

The Tool Chain will be installed automatically on your Linux PC within a few minutes. Before compiling the program, be sure to set the following path first, since the Tool Chain files, including the compiler, link, library, and include files are located in this directory.

```
PATH=/usr/local/arm-linux/bin:$PATH
```

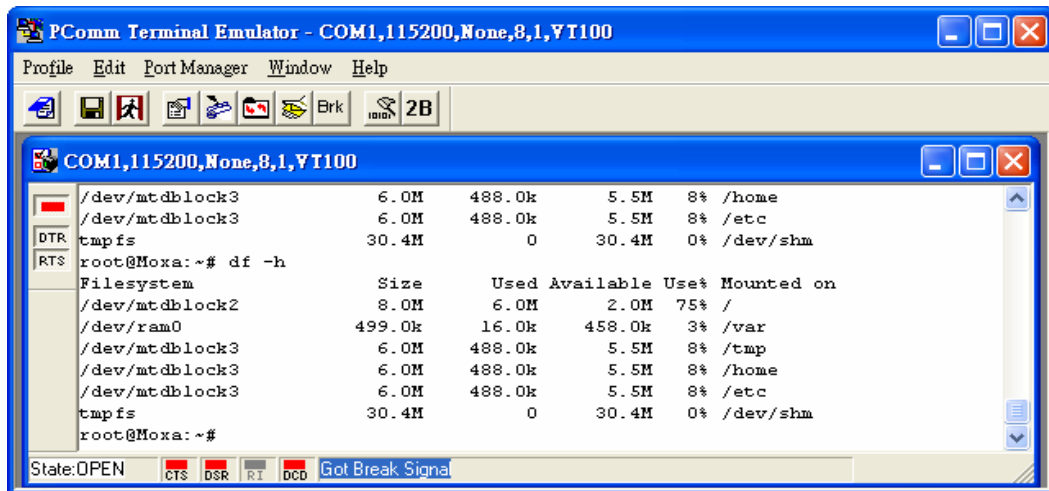
Setting the path allows you to run the compiler from any directory.

NOTE Refer to Appendix B for an introduction to the Windows Tool Chain. In this chapter, we use the Linux tool chain to illustrate the cross compiling process.

Checking the Flash Memory Space

If the flash memory is full, you will not be able to save data to the Flash ROM. Use the following command to calculate the amount of “Available” flash memory:

```
/>df -h
```



If there isn't enough "Available" space for your application, you will need to delete some existing files. To do this, connect your PC to the W311/321/341 with the console cable, and then use the console utility to delete the files from the W311/321/341's flash memory. To check the amount of free space available, look at the directories in the read/write directory `/dev/mtdblock3`. Note that the directories `/home` and `/etc` are both mounted on the directory `/dev/mtdblock3`.

NOTE If the flash memory is full, you will need to free up some memory space before saving files to the Flash ROM.

Compiling Hello.c

The package CD contains several example programs. Here we use **Hello.c** as an example to show you how to compile and run your applications. Type the following commands from your PC to copy the files used for this example from the CD to your computer's hard drive:

```
# cd /tmp/
# mkdir example
# cp -r /mnt/cdrom/example/* /tmp/example
```

To compile the program, go to the **Hello** subdirectory and issue the following commands:

```
#cd example/hello
#make
```

You should receive the following response:

```
[root@localhost hello]# make
/usr/local/arm-linux/bin/arm-linux-gcc -o hello-release hello.c
/usr/local/arm-linux/bin/arm-linux-strip -s hello-release
/usr/local/arm-linux/bin/arm-linux-gcc -ggdb -o hello-debug hello.c
[root@localhost hello]# _
```

Next, execute **make** to generate **hello-release** and **hello-debug**, which are described below:

hello-release—an ARM platform execution file (created specifically to run on the W311/321/341)

hello-debug—an ARM platform GDB debug server execution file (see Chapter 5 for details about the GDB debug tool).

NOTE Since Moxa's tool chain places a specially designed **Makefile** in the directory `/tmp/example/hello`, be sure to type the `#make` command from within that directory. This special Makefile uses the `mxscale-gcc` compiler to compile the `hello.c` source code for the Xscale environment. If you type the `#make` command from within any other directory, Linux will use the x86 compiler (for example, `cc` or `gcc`).

Refer to Chapter 5 to see a Makefile example.

Uploading and Running the "Hello" Program

Use the following commands to upload **hello-release** to the W311/321/341 by FTP.

1. From the PC, type:

```
#ftp 192.168.3.127
```

2. Use the `bin` command to set the transfer mode to Binary mode, and then use the `put` command to initiate the file transfer:

```
ftp> bin
ftp> cd /home
ftp> put hello-release
```

3. From the W311/321/341, type:

```
# chmod +x hello-release
# ./hello-release
```

The word **Hello** will be printed on the screen.

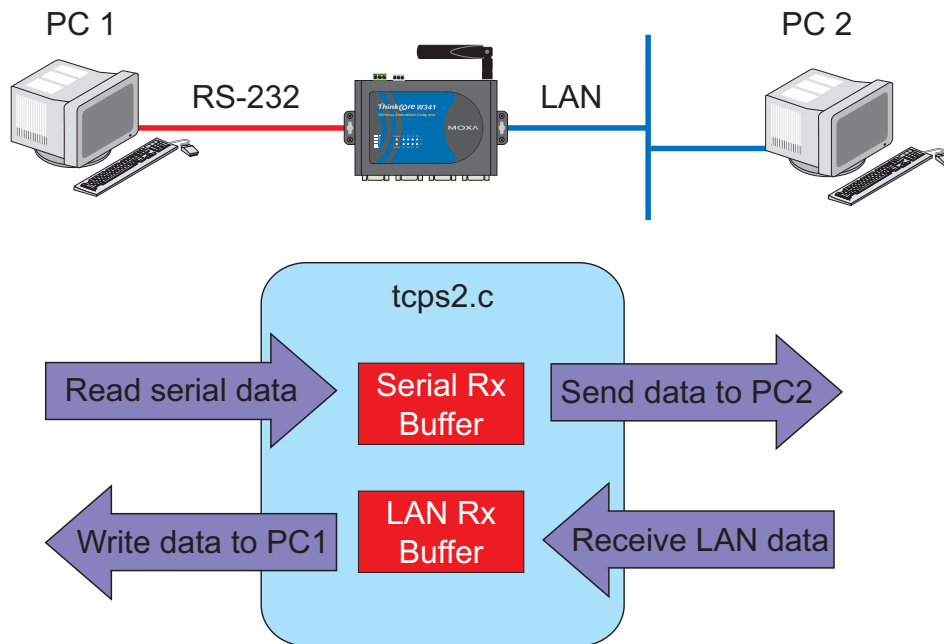
```
root@Moxa:~# ./hello-release
Hello
```

Developing Your First Application

We use the `tcps2` example to illustrate how to build an application. The procedure outlined in the following subsections will show you how to build a TCP server program plus serial port communication that runs on the W311/321/341.

Testing Environment

The `tcps2` example demonstrates a simple application program that delivers transparent, bi-directional data transmission between the W311/321/341's serial and Ethernet ports. As illustrated in the following figure, the purpose of this application is to transfer data between PC 1 and the W311/321/341 through an RS-232 connection. At the remote site, data can be transferred between the W311/321/341's Ethernet port and PC 2 over an Ethernet connection.



Compiling tcps2.c

The source code for the tcps2 example is located on the CD-ROM at **CD-ROM://example/TCPServer2/tcps2.c**. Use the following commands to copy the file to a specific directory on your PC. We use the directory **/home/w341/1st_application/**. Note that you need to copy 3 files—**Makefile**, **tcps2.c**, **tcpsp.c**—from the CD-ROM to the target directory.

```
#mount -t iso9660 /dev/cdrom /mnt/cdrom
#cp /mnt/cdrom/example/TCPServer2/tcps2.c/home/w341/1st_application/tcps2.c
#cp /mnt/cdrom/example/TCPServer2/tcpsp.c/home/w341/1st_application/tcpsp.c
#cp /mnt/cdrom/example/TCPServer2/Makefile.c/home/w341/1st_application/Makefile
```

Type **#make** to compile the example code:

You will get the following response, indicating that the example program was compiled successfully.

```
root@server11: /home/w341/1st_application
[root@server11 1st_application]# pwd
/home/w341/1st_application
[root@server11 1st_application]# ll
total 20
-rw-r--r-- 1 root root 514 Nov 27 11:52 Makefile
-rw-r--r-- 1 root root 4554 Nov 27 11:52 tcps2.c
-rw-r--r-- 1 root root 6164 Nov 27 11:55 tcpsp.c
[root@server11 1st_application]# make_
/usr/local/arm-linux/bin/arm-linux-gcc -o tcps2-release tcps2.c
/usr/local/arm-linux/bin/arm-linux-strip -s tcps2-release
/usr/local/arm-linux/bin/arm-linux-gcc -o tcpsp-release tcpsp.c
/usr/local/arm-linux/bin/arm-linux-strip -s tcpsp-release
/usr/local/arm-linux/bin/arm-linux-gcc -ggdb -o tcps2-debug tcps2.c
/usr/local/arm-linux/bin/arm-linux-gcc -ggdb -o tcpsp-debug tcpsp.c
[root@server11 1st_application]# ll
total 92
-rw-r--r-- 1 root root 514 Nov 27 11:52 Makefile
-rwxr-xr-x 1 root root 25843 Nov 27 12:03 tcps2-debug
-rwxr-xr-x 1 root root 4996 Nov 27 12:03 tcps2-release
-rw-r--r-- 1 root root 4554 Nov 27 11:52 tcps2.c
-rwxr-xr-x 1 root root 26823 Nov 27 12:03 tcpsp-debug
-rwxr-xr-x 1 root root 5396 Nov 27 12:03 tcpsp-release
-rw-r--r-- 1 root root 6164 Nov 27 11:55 tcpsp.c
[root@server11 1st_application]# █
```

Two executable files, **tcps2-release** and **tcps2-debug**, are created.

tcps2-release—an ARM platform execution file (created specifically to run on the W311/321/341).

tcps2-debug—an ARM platform GDB debug server execution file (see Chapter 5 for details about the GDB debug tool).

| | |
|------|---|
| NOTE | If you get an error message at this point, it could be because you neglected to put tcps2.c and tcpsp.c in the same directory. The example Makefile we provide is set up to compile both tcps2 and tcpsp into the same project Makefile . Alternatively, you could modify the Makefile to suit your particular requirements. |
|------|---|

Uploading and Running the “tcps2-release” Program

Use the following commands to upload **tcps2-release** to the W311/321/341 through an FTP connection.

1. From the PC, type:

```
#ftp 192.168.3.127
```

2. Next, use the **bin** command to set the transfer mode to **Binary**, and the **put** command to initiate the file transfer:

```
ftp> bin
ftp> cd /home
ftp> put tcps2-release
```

```
root@server11:/home/w341/1st_application
[root@server11 1st_application]# ftp 192.168.3.127
Connected to 192.168.3.127
220 Moxa FTP server (Version wu-2.6.1(2) Mon Nov 24 12:17:04 CST 2003) ready.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS V4 rejected as an authentication type
Name (192.168.3.127:root): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I.
ftp> put tcps2-release
local: tcps2-release remote: tcps2-release
277 Entering Passive Mode (192.168.3.127.82.253)
150 Opening BINARY mode data connection for tcps2-release.
226 Transfer complete
4996 bytes sent in 0.00013 seconds (3.9e+04 Kbytes/s)
ftp> ls
227 Entering Passive Mode (192.168.3.127.106.196)
150 Opening ASCII mode data connection for /bin/ls.
-rw----- 1 root root 899 Jun 10 08:11 bash history
-rw-r--r-- 1 root root 4996 Jun 12 02:15 tcps2-release
226 Transfer complete
ftp>
```

3. From the W311/321/341, type:

```
# chmod +x tcps2-release
# ./tcps2-release &
```

```
192.168.3.127 - PuTTY
root@Moxa:~# ls -al
drwxr-xr-x 2 root root 0 Jun 12 02:14
drwxr-xr-x 15 root root 0 Jan 1 1970
-rw----- 1 root root 899 Jun 10 08:11 .bash history
-rw-r--r-- 1 root root 4996 Jun 12 02:15 tcps2-release
root@Moxa:~# chmod +x tcps2-release
root@Moxa:~# ls -al
drwxr-xr-x 2 root root 0 Jun 12 02:14
drwxr-xr-x 15 root root 0 Jan 1 1970
-rw----- 1 root root 899 Jun 10 08:11 .bash history
-rwxr-xr-x 1 root root 4996 Jun 12 02:15 tcps2-release
root@Moxa:~#
```

- The program should start running in the background. Use the `#ps -ef` command to check if the `tcps2` program is actually running in the background.

`#ps // use this command to check if the program is running`

```
192.168.3.127 - PuTTY
root@Moxa:~# ls -al
drwxr-xr-x 2 root root 0 Jun 12 02:14
drwxr-xr-x 15 root root 0 Jan 1 1970
-rw----- 1 root root 899 Jun 10 08:11 .bash_history
-rw-r--r-- 1 root root 4996 Jun 12 02:15 tcps2-release
root@Moxa:~# chmod +x tcps2-release
root@Moxa:~# ls -al
drwxr-xr-x 2 root root 0 Jun 12 02:14
drwxr-xr-x 15 root root 0 Jan 1 1970
-rw----- 1 root root 899 Jun 10 08:11 .bash_history
-rwxr-xr-x 1 root root 4996 Jun 12 02:15 tcps2-release
root@Moxa:~# ./tcps2-release &
[1] 187
start
root@Moxa:~# ps
[1]+  Running ./tcps2-release &
root@Moxa:~# █
```

NOTE Use the `kill` command for job number 1 to terminate this program: `#kill %1`

`#ps -ef // use this command to check if the program is running`

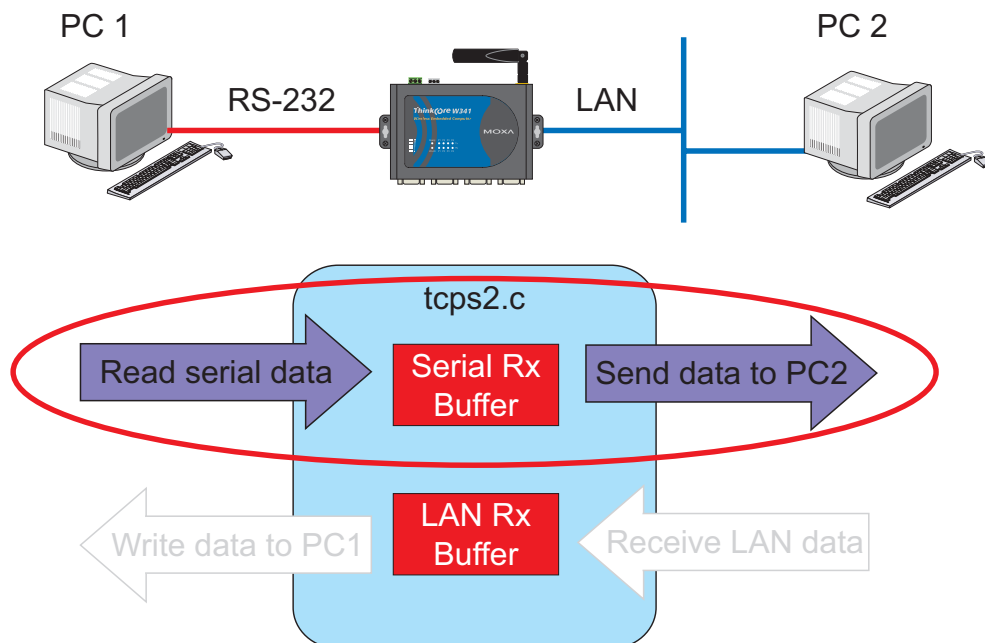
```
192.168.3.127 - PuTTY
[1]+  Running ./tcps2-release &
root@Moxa:~# ps -ef
PID Uid  VmSize Stat Command
  1 root    532 S  init [3]
  2 root          SWN [ksoftirqd/0]
  3 root          SW< [events/0]
  4 root          SW< [khelper]
 13 root          SW< [kblockd/0]
 14 root          SW [khubd]
 24 root          SW [pdflush]
 25 root          SW [pdflush]
 27 root          SW< [aio/0]
 26 root          SW [kswapd0]
604 root          SW [mtdblockd]
609 root          SW [pccardd]
611 root          SW [pccardd]
625 root          SWN [jffs2_gcd_mtd3]
673 root    500 S  /bin/inetd
679 root   3004 S  /usr/bin/httpd -k start -d /etc/apache
682 bin     380 S  /bin/portmap
685 root   1176 S  /bin/sh --login
690 root    464 S  /bin/snmpd
694 nobody 3012 S  /usr/bin/httpd -k start -d /etc/apache
695 nobody 3012 S  /usr/bin/httpd -k start -d /etc/apache
696 nobody 3012 S  /usr/bin/httpd -k start -d /etc/apache
697 nobody 3012 S  /usr/bin/httpd -k start -d /etc/apache
698 nobody 3012 S  /usr/bin/httpd -k start -d /etc/apache
701 root    352 S  /bin/reportip
714 root   1176 S  -bash
726 root    436 S  /bin/telnetd
727 root   1164 S  -bash
728 root   1264 S  ./tcps2-release
729 root   1592 S  ps -ef
root@Moxa:~# █
```

NOTE Use the `kill -9` command for PID 728 to terminate this program: `#kill -9 %728`

Testing Procedure Summary

1. Compile `tcps2.c` (`#make`).
2. Upload and run `tcps2-release` in the background (`#!/tcps2-release &`).
3. Check that the process is running (`#jobs` or `#ps -ef`).
4. Use a serial cable to connect PC1 to the W311/321/341's serial port 1.
5. Use an Ethernet cable to connect PC2 to the W311/321/341.
6. On PC1: If running Windows, use HyperTerminal (**38400, n, 8, 1**) to open COMn.
7. On PC2: Type `#telnet 192.168.3.127 4001`.
8. On PC1: Type some text on the keyboard and then press **Enter**.
9. On PC2: The text you typed on PC1 will appear on PC2's screen.

The testing environment is illustrated in the following figure. However, note that there are limitations to the example program `tcps2.c`.



NOTE The `tcps2.c` application is a simple example designed to give users a basic understanding of the concepts involved in combining Ethernet communication and serial port communication. However, the example program has some limitations that make it unsuitable for real-life applications.

1. The serial port is in canonical mode and block mode, making it impossible to send data from the Ethernet side to the serial side (i.e., from PC 2 to PC 1 in the above example).
2. The Ethernet side will not accept multiple connections.

Managing Embedded Linux

This chapter includes information about version control, deployment, updates, and peripherals. The information in this chapter will be particularly useful when you need to run the same application on several W311/321/341 units.

The following topics are covered in this chapter:

- ❑ **System Version Information**
- ❑ **System Image Backup**
 - Upgrading the Firmware
 - Loading Factory Defaults
 - Backing Up the User Directory
 - Deploying the User Directory to Additional W311/321/341 Units
- ❑ **Enabling and Disabling Daemons**
- ❑ **Setting the Run-Level**
- ❑ **Adjusting the System Time**
 - Setting the Time Manually
 - NTP Client
 - Updating the Time Automatically
- ❑ **Cron—daemon to Execute Scheduled Commands**

System Version Information

To determine the hardware capability of your W311/321/341, and what kind of software functions are supported, check the version numbers of your W311/321/341's hardware, kernel, and user file system. Contact Moxa to determine the hardware version. You will need the **Production S/N** (Serial number), which is located on the W311/321/341's bottom label.

To check the kernel version, type:

```
#kversion
```

```
192.168.3.127 - PuTTY
root@moxa:~# kversion
Version 1.0
root@moxa:~# █
```

NOTE The kernel version number is for the factory default configuration. You may download the latest firmware version from Moxa's website and then upgrade the W311/321/341's hardware.

System Image Backup

Upgrading the Firmware

The W311/321/341's bios, kernel, and root file system are combined into one firmware file, which can be downloaded from Moxa's website (www.moxa.com). The name of the file has the form **w341-x.x.x.frm**, with "x.x.x" indicating the firmware version. To upgrade the firmware, download the firmware file to a PC, and then transfer the file to the W311/321/341 using a console port or Telnet console connection.



ATTENTION

Upgrading the firmware will erase all data on the Flash ROM

If you are using the **ramdisk** to store code for your applications, beware that updating the firmware will erase all of the data on the Flash ROM. You should back up your application files and data before updating the firmware.

Since different Flash disks have different sizes, it is a good idea to check the size of your Flash disk before upgrading the firmware, or before using the disk to store your application and data files. Use the `df -h` command to list the size of each memory block and how much free space is available in each block.

```
192.168.3.127 - PuTTY
root@Moxa:~# df -h
Filesystem      Size  Used Available Use% Mounted on
/dev/mtdblock2 8.0M   6.0M   2.0M   75% /
/dev/ram0       499.0k 16.0k  458.0k   3% /var
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /tmp
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /home
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /etc
tmpfs          30.4M   0      30.4M   0% /dev/shm
root@Moxa:~# upramdisk
root@Moxa:~# df -h
Filesystem      Size  Used Available Use% Mounted on
/dev/mtdblock2 8.0M   6.0M   2.0M   75% /
/dev/ram0       499.0k 16.0k  458.0k   3% /var
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /tmp
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /home
/dev/mtdblock3 6.0M   488.0k 5.5M    8% /etc
tmpfs          30.4M   0      30.4M   0% /dev/shm
/dev/ram1      16.0M   1.0k  15.1M   0% /mnt/ramdisk
root@Moxa:~# cd /mnt/ramdisk
root@Moxa:/mnt/ramdisk#
```

The following instructions give the steps required to save the firmware file to the W311/321/341's RAM disk and how to upgrade the firmware.

1. Type the following commands to enable the RAM disk:

```
#upramdisk
#cd /mnt/ramdisk
```


2. Type the following commands to use the W311/321/341's built-in FTP client to transfer the firmware file (W341-x.x.x.frm) from the PC to the W311/321/341:

```
/mnt/ramdisk> ftp <destination PC's IP>
Login Name: xxxx
Login Password: xxxx
ftp> bin
ftp> get -x.x.x.frm
```

```
192.168.3.127 - PuTTY
root@Moxa:/mnt/ramdisk# ftp 192.168.3.193
Connected to 192.168.3.193 (192.168.3.193).
220 TYPSoft FTP Server 1.10 ready...
Name (192.168.3.193:root): root
331 Password required for root.
Password:
230 User root logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd newsw
250 CWD command successful. "/C:/ftproot/newsw/" is current directory.
ftp> bin
200 Type set to I.
ftp> ls
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-  1 ftp ftp    0 Nov 30 10:03 .
drw-rw-rw-  1 ftp ftp    0 Nov 30 10:03 .
-rw-rw-rw-  1 ftp ftp 13167772 Nov 29 10:24 w3xx-1.0.frm
226 Transfer complete.
ftp> get w3xx-1.0.frm
local: ia240-1.0.frm remote: w3xx-1.0.frm
200 Port command successful.
150 Opening data connection for w3xx-1.0.frm
226 Transfer complete.
13167772 bytes received in 2.17 secs (5925.8 kB/s)
ftp> █
```

3. Next, use the **upfirm** command to upgrade the kernel and root file system:

```
#upfirm w3xx-x.x.x.frm
```

```
192.168.3.127 - PuTTY
root@Moxa:/mnt/ramdisk# upfirm w3xx-1.0.frm
Moxa ThinkCore IA240 upgrade firmware utility version 1.0.
To check source firmware file context.
The source firmware file context is OK.
This step will destroy all your firmware.
Continue ? (Y/N) : Y
Now upgrade the file [kernel].
Format MTD device [/dev/mtd1] . . .
MTD device [/dev/mtd1] erase 128 Kibyte @ 1C0000 - 100% complete.
Wait to write file . . .
Completed 100%
Now upgrade the file [usrdisk].
Format MTD device [/dev/mtd2] . . .
MTD device [/dev/mtd2] erase 128 Kibyte @ 800000 - 100% complete.
Wait to write file . . .
Completed 100%
Upgrade the firmware is OK.
```

**ATTENTION**

The upfirm utility will reboot your target after the upgrade is OK.

Loading Factory Defaults

To load the the factory default settings, you must press the reset-to-default button for more than 5 seconds. All files in the /home & /etc directories will be destroyed. Note that while pressing the reset-to-default button, the Ready LED will blink once every second for the first 5 seconds. The Ready LED will turn off after 5 seconds, and the factory defaults will be loaded.

Backing Up the User Directory

1. Create a backup file. First type the following command to enable the RAM disk:
`#upramdisk`

Next, use the file system backup utility provided by Moxa:

```
#backupuf /mnt/ramdisk/usrfs-backup
```

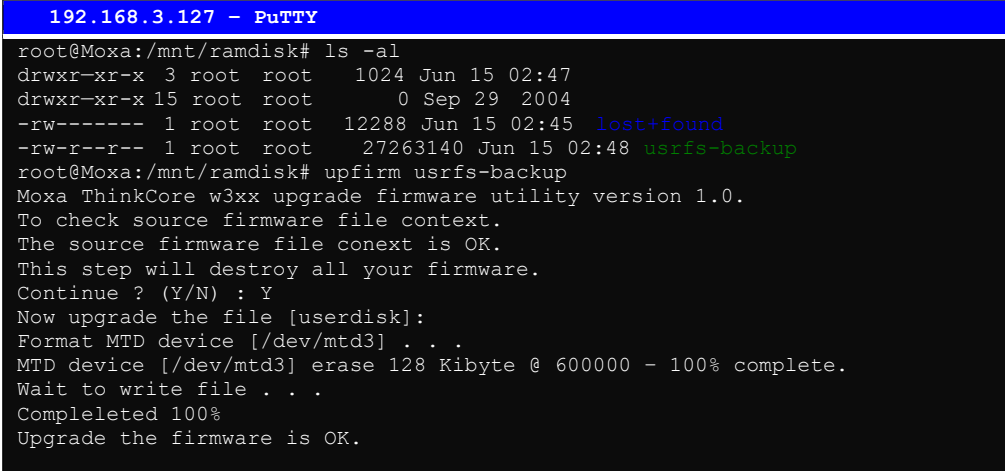
2. Once the file system is backed up, use FTP to transfer the file **usrfs-backup** to your PC.

```
192.168.3.127 - PuTTY
root@Moxa:~# upramdisk
root@Moxa:~# cd /mnt/ramdisk
root@Moxa:/mnt/ramdisk# df -h
Filesystem      Size      Used Available Use% Mounted on
/dev/mtdblock2  8.0M      6.0M    2.0M    75% /
/dev/ram0        499.0k    17.0k  457.0k    4% /var
/dev/mtdblock3  6.0M     488.0k   5.5M    8% /tmp
/dev/mtdblock3  6.0M     488.0k   5.5M    8% /home
/dev/mtdblock3  6.0M     488.0k   5.5M    8% /etc
tmpfs           30.4M      0    30.4M    0% /dev/shm
/dev/ram1       16.0M      1.0k  15.1M    0% /var/ramdisk
root@Moxa:/mnt/ramdisk# backupuf /mnt/ramdisk/usrfs-backup
Sync the file system...
Now backup the user root file system. Please wait. . .
. . . . .
Backup user root file system OK.
root@Moxa:/mnt/ramdisk#
```

Deploying the User Directory to Additional W311/321/341 Units

For some applications, you may need to ghost one W311/321/341 user file system to other W311/321/341 units. Back up the user file system to a PC (refer to the previous subsection, *Backing Up the User File System*, for instructions), and then type the following commands to copy the backup to additional W311/321/341 units.

```
#upramdisk
#cd /mnt/ramdisk
#upfirm usrfs-backup
```



```
192.168.3.127 - PuTTY
root@Moxa:/mnt/ramdisk# ls -al
drwxr-xr-x 3 root root 1024 Jun 15 02:47
drwxr-xr-x 15 root root 0 Sep 29 2004
-rw----- 1 root root 12288 Jun 15 02:45 lost+found
-rw-r--r-- 1 root root 27263140 Jun 15 02:48 usrfs-backup
root@Moxa:/mnt/ramdisk# upfirm usrfs-backup
Moxa ThinkCore w3xx upgrade firmware utility version 1.0.
To check source firmware file context.
The source firmware file context is OK.
This step will destroy all your firmware.
Continue ? (Y/N) : Y
Now upgrade the file [userdisk]:
Format MTD device [/dev/mtd3] . . .
MTD device [/dev/mtd3] erase 128 Kibyte @ 600000 - 100% complete.
Wait to write file . . .
Completed 100%
Upgrade the firmware is OK.
```

Enabling and Disabling Daemons

The following daemons are enabled when the W311/321/341 unit boots up for the first time.

```
snmpd .....SNMP Agent daemon
telnetd .....Telnet Server / Client daemon
inetd .....Internet Daemons
ftpd.....FTP Server / Client daemon
sshd .....Secure Shell Server daemon
httpd .....Apache WWW Server daemon
```

Type the command “ps -ef” to list all processes currently running.

```

192.168.3.127 - PuTTY
root@Moxa:~# cd /etc
root@Moxa:/etc# ps -ef
PID  Uid    VmSize  Stat  Command
   1  root      532  S    init [3]
   2  root          SWN  [ksoftirqd/0]
   3  root          SW<  [events/0]
   4  root          SW<  [khelper]
  13  root          SW<  [kblockd/0]
  14  root          SW    [khubd]
  24  root          SW    [pdflush]
  25  root          SW    [pdflush]
  27  root          SW<  [aio/0]
  26  root          SW    [kswapd0]
 604  root          SW    [mtdblockd]
 609  root          SW    [pccardd]
 611  root          SW    [pccardd]
 625  root          SWN  [jffs2_gcd_mtd3]
 673  root      500  S    /bin/inetd
 679  root     3004  S    /usr/bin/httpd -k start -d /etc/apache
 682  bin       380  S    /bin/portmap
 685  root     1176  S    /bin/sh --login
 690  root      464  S    /bin/snmpd
 694  nobody   3012  S    /usr/bin/httpd -k start -d /etc/apache
 695  nobody   3012  S    /usr/bin/httpd -k start -d /etc/apache
 696  nobody   3012  S    /usr/bin/httpd -k start -d /etc/apache
 697  nobody   3012  S    /usr/bin/httpd -k start -d /etc/apache
 698  nobody   3012  S    /usr/bin/httpd -k start -d /etc/apache
 701  root      352  S    /bin/reportip
 714  root     1176  S    -bash
 726  root      436  S    /bin/telnetd
 727  root     1180  S    -bash
 783  root      628  R    ps -ef
root@Moxa:/ect# █

```

To run a private daemon, you can edit the file rc.local, as follows:

```
#cd /etc/rc.d
#vi rc.local
```

```

192.168.3.127 - PuTTY
root@Moxa:~# cd /etc/rc.d
root@Moxa:/etc/rc.d# vi rc.local █

```

Next, use vi to open your application program. We use the example program **tcps2-release**, and put it to run in the background.

```

192.168.3.127 - PuTTY
# !/bin/sh
# Add you want to run daemon
/home/tcps2-release &~

```

The enabled daemons will be available after you reboot the system.

```

192.168.3.127 - PuTTY
root@Moxa:~# ps -ef
  PID  Uid    VmSize  Stat Command
    1  root      532 S    init [3]
    2  root          SWN  [ksoftirqd/0]
    3  root          SW<  [events/0]
    4  root          SW<  [khelper]
   13  root          SW<  [kblockd/0]
   14  root          SW   [khubd]
   24  root          SW   [pdflush]
   25  root          SW   [pdflush]
   27  root          SW<  [aio/0]
   26  root          SW   [kswapd0]
  604  root          SW   [mtdblockd]
  609  root          SW   [pccardd]
  611  root          SW   [pccardd]
  625  root          SWN  [jffs2_gcd_mtd3]
  673  root      500 S    /bin/inetd
  674  root     1264 S    /root/tcps2-release
  679  root     3004 S    /usr/bin/httpd -k start -d /etc/apache
  682  bin       380 S    /bin/portmap
  685  root     1176 S    /bin/sh --login
  690  root      464 S    /bin/snmpd
  694  nobody   3012 S    /usr/bin/httpd -k start -d /etc/apache
  695  nobody   3012 S    /usr/bin/httpd -k start -d /etc/apache
  696  nobody   3012 S    /usr/bin/httpd -k start -d /etc/apache
  697  nobody   3012 S    /usr/bin/httpd -k start -d /etc/apache
  698  nobody   3012 S    /usr/bin/httpd -k start -d /etc/apache
  701  root      352 S    /bin/reportip
  714  root     1176 S    -bash
  726  root      436 S    /bin/telnetd
  727  root     1180 S    -bash
  783  root      628 R    ps -ef
root@Moxa:~#

```

Setting the Run-Level

In this section, we outline the steps you should take to set the Linux run-level and execute requests. Use the following command to enable or disable settings:

```

192.168.3.127 - PuTTY
root@Moxa:/etc/rc.d/rc3.d# ls
S19nfs-common S25nfs-user-serverS99showreadyled
S20snmpd      S55ssh
S24pcmcia    S99rmnologin
root@Moxa:/etc/rc.d/rc3.d#

```

```
#cd /etc/rc.d/init.d
```

Edit a shell script to execute `/home/tcps2-release` and save to `tcps2` as an example.

```
#cd /etc/rc.d/rc3.d
```

```
#ln -s /etc/rc.d/init.d/tcps2 S60tcps2
```

SxxRUNFILE stands for

S: start the run file while linux boots up.

xx: a number between 00-99. Smaller numbers have a higher priority.

RUNFILE: the file name.

```
192.168.3.127 - PuTTY
root@Moxa:/etc/rc.d/rc3.d# ls
S19nfs-common S25nfs-user-serverS99showreadyled
S20snmpd S55ssh
S24pcmcia S99rmnologin
root@Moxa:/etc/rc.d/rc3.d# ln -s /home/tcps2-release S60tcps2
root@Moxa:/etc/rc.d/rc3.d# ls
S19nfs-common S25nfs-user-serverS99rmnologin
S20snmpd S55ssh S99showreadyled
S24pcmcia S60tcps2
root@Moxa:/etc/rc.d/rc3.d# █
```

KxxRUNFILE stands for

K: start the run file while linux shuts down or halts.

xx: a number between 00-99. Smaller numbers have a higher priority.

RUNFILE: the file name.

To remove the daemon, remove the run file from the `/etc/rc.d/rc3.d` directory by using the following command:

```
#rm -f /etc/rc.d/rc3.d/S60tcps2
```

Adjusting the System Time

Setting the Time Manually

The W311/321/341 have two time settings. One is the system time, and the other is the RTC (Real Time Clock) time kept by the W311/321/341's hardware. Use the `#date` command to query the current system time or set a new system time. Use `#hwclock` to query the current RTC time or set a new RTC time.

Use the following command to query the system time:

```
#date
```

Use the following command to query the RTC time:

```
#hwclock
```

Use the following command to set the system time:

```
#date MMDDhhmmYYYY
```

MM = Month

DD = Date

hhmm = hour and minute

YYYY = Year

Use the following command to set the RTC time:

```
#hwclock -w
```

Write current system time to RTC

The following figure illustrates how to update the system time and set the RTC time.

```

192.168.3.127 - PuTTY
root@Moxa:~# date
Fri Jun 23 23:30:31 CST 2000
root@Moxa:~# hwclock
Fri Jun 23 23:30:35 2000 -0.557748 seconds
root@Moxa:~# date 120910002004
Thu Dec 9 10:00:00 CST 2004
root@Moxa:~# hwclock -w
root@Moxa:~# date ; hwclock
Thu Dec 9 10:01:07 CST 2004
Thu Dec 9 10:01:08 2004 -0.933547 seconds
root@Moxa:~# █

```

NTP Client

The W311/321/341 have a built-in NTP (Network Time Protocol) client that is used to initialize a time request to a remote NTP server. Use `#ntpdate <this client utility>` to update the system time.

```
#ntpdate time.stdtime.gov.tw
#hwclock -w
```

Visit <http://www.ntp.org> for more information about NTP and NTP server addresses.

```

10.120.53.100 - PuTTY
root@Moxa:~# date ; hwclock
Sat Jan 1 00:00:36 CST 2000
Sat Jan 1 00:00:37 2000 -0.772941 seconds
root@Moxa:~# ntpdate time.stdtime.gov.tw
9 Dec 10:58:53 ntpdate[207]: step time server 220.130.158.52 offset 155905087.9
84256 sec
root@Moxa:~# hwclock -w
root@Moxa:~# date ; hwclock
Thu Dec 9 10:59:11 CST 2004
Thu Dec 9 10:59:12 2004 -0.844076 seconds
root@Moxa:~# █

```

NOTE Before using the NTP client utility, check your IP and DNS settings to make sure that an Internet connection is available. Refer to Chapter 2 for instructions on how to configure the Ethernet interface, and see Chapter 4 for DNS setting information.

Updating the Time Automatically

In this subsection, we show how to use a shell script to update the time automatically.

Example shell script to update the system time periodically

```
#!/bin/sh
ntpdate time.nist.gov # You can use the time server's ip address or domain
# name directly. If you use domain name, you must
# enable the domain client on the system by updating
# /etc/resolv.conf file.
hwclock --systohc
sleep 100 # Updates every 100 seconds. The min. time is 100 seconds. Change
# 100 to a larger number to update RTC less often.
```

Save the shell script using any file name. E.g., `fixtime`

How to run the shell script automatically when the kernel boots up

Copy the example shell script `fixtime` to directory `/etc/init.d`, and then use `chmod 755 fixtime` to change the shell script mode. Next, use vi editor to edit the file `/etc/inittab`. Add the following line to the bottom of the file:

```
ntp : 2345 : respawn : /etc/init.d/fixtime
```

Use the command `#init q` to re-init the kernel.

Cron—Daemon to Execute Scheduled Commands

Start Cron from the directory `/etc/rc.d/rc.local`. It will return immediately, so you don't need to start it with `'&'` to run in the background.

The Cron daemon will search `/etc/cron.d/crontab` for crontab files, which are named after accounts in `/etc/passwd`.

Cron wakes up every minute, and checks each command to see if it should be run in that minute. When executing commands, output is mailed to the owner of the crontab (or to the user named in the MAILTO environment variable in the crontab, if such a user exists).

Modify the file `/etc/cron.d/crontab` to set up your scheduled applications. Crontab files have the following format:

| mm | h | dom | mon | dow | user | command |
|------|------|------|-------|-------------------|------|---------|
| min | hour | date | month | week | user | command |
| 0-59 | 0-23 | 1-31 | 1-12 | 0-6 (0 is Sunday) | | |

The following example demonstrates how to use Cron.

How to use cron to update the system time and RTC time every day at 8:00.**STEP1: Write a shell script named `fixtime.sh` and save it to `/home/`.**

```
#!/bin/sh
ntpdate time.nist.gov
hwclock --systohc
exit 0
```

STEP2: Change mode of `fixtime.sh`

```
#chmod 755 fixtime.sh
```

STEP3: Modify `/etc/cron.d/crontab` file to run `fixtime.sh` at 8:00 every day.

Add the following line to the end of crontab:

```
* 8 * * * root /home/fixtime.sh
```

STEP4: Enable the cron daemon manually.

```
#/etc/init.d/cron start
```

STEP5: Enable cron when the system boots up.

Add the following line in the file `/etc/init.d/rc.local`

```
#/etc/init.d/cron start
```


Managing Communications

In this chapter, we explain how to configure the W311/321/341's various communication functions.

The following topics are covered in this chapter:

- Telnet / FTP**
- DNS**
- Web Service—Apache**
- Installing PHP for Apache Web Service**
- IPTABLES**
- NAT**
 - NAT Example
 - Enabling NAT at Bootup
- Dial-up Service—PPP**
- PPPoE**
- NFS (Network File System)**
 - Setting up the W311/321/341 as an NFS Client
- Mail**
- SNMP**
- OpenVPN**

Telnet / FTP

In addition to supporting Telnet client/server and FTP client/server, the W311/321/341 also support SSH and sftp client/server. To enable or disable the Telnet/ftp server, you first need to edit the file `/etc/inetd.conf`.

Enabling the Telnet/ftp server

The following example shows the default content of the file `/etc/inetd.conf`. The default is to enable the Telnet/ftp server:

```
discard dgram udp wait root /bin/discard
discard stream tcp nowait root /bin/discard
telnet stream tcp nowait root /bin/telnetd
ftp stream tcp nowait root /bin/ftpd -l
```

Disabling the Telnet/ftp server

Disable the daemon by typing '#' in front of the first character of the row to comment out the line.

DNS

The W311/321/341 support DNS client (but not DNS server). To set up DNS client, you need to edit three configuration files: `/etc/hosts`, `/etc/resolv.conf`, and `/etc/nsswitch.conf`.

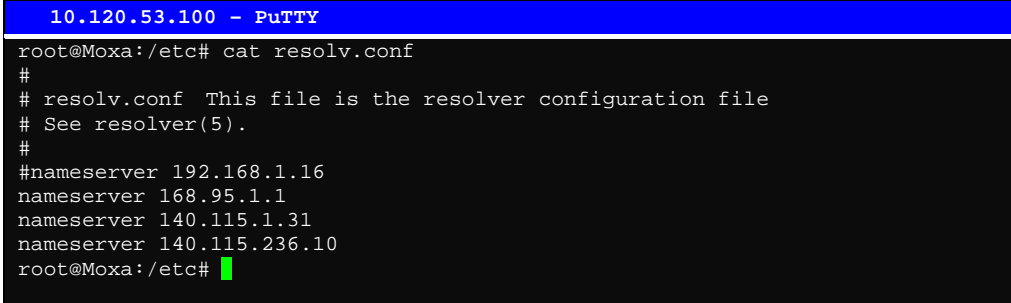
`/etc/hosts`

This is the first file that the Linux system reads to resolve the host name and IP address.

`/etc/resolv.conf`

This is the most important file that you need to edit when using DNS for the other programs. For example, before you use `#ntpdate time.nist.gov` to update the system time, you will need to add the DNS server address to the file. Ask your network administrator which DNS server address you should use. The DNS server's IP address is specified with the "nameserver" command. For example, add the following line to `/etc/resolv.conf` if the DNS server's IP address is 168.95.1.1:

```
nameserver 168.95.1.1
```



```
10.120.53.100 - PuTTY
root@Moxa:/etc# cat resolv.conf
#
# resolv.conf This file is the resolver configuration file
# See resolver(5).
#
#nameserver 192.168.1.16
nameserver 168.95.1.1
nameserver 140.115.1.31
nameserver 140.115.236.10
root@Moxa:/etc#
```

`/etc/nsswitch.conf`

This file defines the sequence to resolve the IP address by using `/etc/hosts` file or `/etc/resolv.conf`.

Web Service—Apache

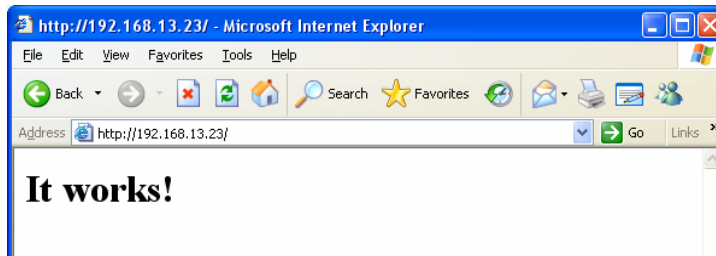
The Apache web server's main configuration file is `/etc/apache/conf/httpd.conf`, with the default homepage located at `/home/httpd/htdocs/index.html`. Save your own homepage to the following directory:

`/home/httpd/htdocs/`

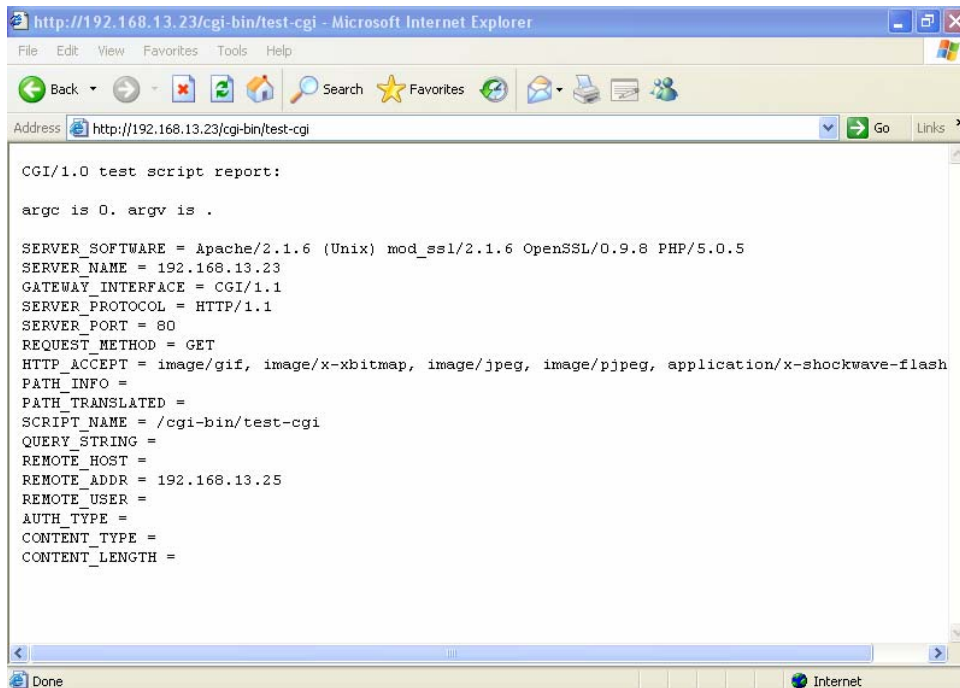
Save your CGI page to the following directory:

/home/httpd/cgi-bin/

Before you modify the homepage, use a browser (such as Microsoft Internet Explorer or Mozilla Firefox) from your PC to test if the Apache Web Server is working. Type the LAN1 IP address in the browser's address box to open the homepage. E.g., if the default IP address is still active, type **http://192.168.3.127** in the address box.



To open the default CGI page, type **http://192.168.3.127/cgi-bin/test-cgi** in your browser's address box.



To open the default CGI test script report page, type **http://192.168.3.127/cgi-bin/test-cgi** in your browser's address box.



```

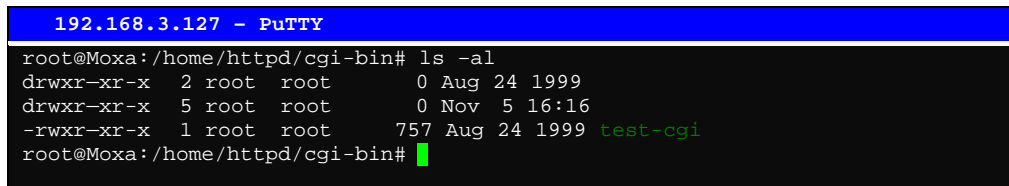
Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.3.127/cgi-bin/test-cgi
Getting Started Latest Headlines
CGI/1.0 test script report:

argc is 0. argv is .

SERVER_SOFTWARE = Apache/2.0.42 (Unix)
SERVER_NAME = localhost
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.1
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT = text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi-bin/test-cgi
QUERY_STRING =
REMOTE_HOST =
REMOTE_ADDR = 192.168.3.105
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =

```

NOTE The CGI function is enabled by default. If you want to disable the function, modify the file **/etc/apache/conf/httpd.conf**. When you develop your own CGI application, make sure your CGI file is executable.



```

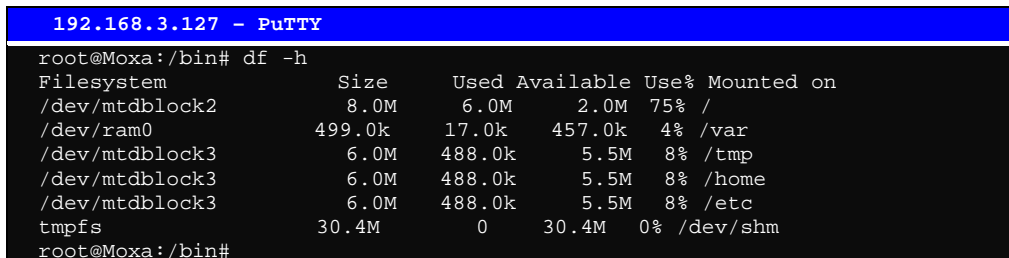
192.168.3.127 - PuTTY
root@Moxa: /home/httpd/cgi-bin# ls -al
drwxr-xr-x  2 root  root    0 Aug 24 1999
drwxr-xr-x  5 root  root    0 Nov  5 16:16
-rwxr-xr-x  1 root  root   757 Aug 24 1999 test-cgi
root@Moxa: /home/httpd/cgi-bin#

```

Installing PHP for Apache Web Server

This embedded computer supports the PHP option. However, since the PHP file is 3 MB, it is not installed by default. To install it yourself, first make sure there is enough free space (at least 3 MB) on your embedded flash ROM).

Step 1: Check that you have enough free space



```

192.168.3.127 - PuTTY
root@Moxa: /bin# df -h
Filesystem      Size      Used Available Use% Mounted on
/dev/mtdblock2  8.0M       6.0M       2.0M   75% /
/dev/ram0       499.0k     17.0k     457.0k    4% /var
/dev/mtdblock3  6.0M     488.0k     5.5M    8% /tmp
/dev/mtdblock3  6.0M     488.0k     5.5M    8% /home
/dev/mtdblock3  6.0M     488.0k     5.5M    8% /etc
tmpfs          30.4M       0       30.4M    0% /dev/shm
root@Moxa: /bin#

```

To check that the **/dev/mtdblock3** free space is greater than 3 MB.

Step 2: Type 'upramdisk' to get the free space ram disk to save the package.

```
192.168.3.127 - PuTTY
root@Moxa:/bin# upramdisk
root@Moxa:/bin# df -h
Filesystem      Size      Used Available Use% Mounted on
/dev/mtdblock2  8.0M      6.0M      2.0M   75% /
/dev/ram0       499.0k    18.0k    456.0k   4% /var
/dev/mtdblock3  6.0M     488.0k    5.5M    8% /tmp
/dev/mtdblock3  6.0M     488.0k    5.5M    8% /home
/dev/mtdblock3  6.0M     488.0k    5.5M    8% /etc
tmpfs           30.4M      0        30.4M   0% /dev/shm
/dev/ram1       16.0M      1.0k     15.1M   0% /var/ramdisk
root@Moxa:/bin#
```

Step 3: Download the PHP package from the CD-ROM. You can find the package in CD-ROM/target/php/php.tar.gz

```
192.168.3.127 - PuTTY
root@Moxa:/bin# cd /mnt/ramdisk
root@Moxa:/mnt/ramdisk# ftp 192.168.27.130
Connected to 192.168.27.130.
220 (vsFTPD 2.0.1)
Name (192.168.27.130:root): root
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /tmp
250 Directory successfully changed.
ftp> bin
200 Switching to Binary mode.
ftp> get php.tar.gz
local: php.tar.gz remote: php.tar.gz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for php.tar.gz (1789032 bytes).
226 File send OK.
1789032 bytes received in 0.66 secs (2.6e+03 Kbytes/sec)
ftp>
```

Step 4: uhtar the package. To do this, type the command 'tar xvzf php.tar.gz'

```
192.168.3.127 - PuTTY
root@Moxa:/mnt/ramdisk# tar xvzf php.tar.gz
envvars
envvars.old
httpd.conf
httpd.conf.old
install.sh
lib
lib/libmysqlclient.so.15
lib/libpng.so.2
lib/libphp5.so
lib/libmysqlclient.so.15.0.0
lib/libgd.so
lib/libxml2.so.2.6.22
lib/libgd.so.2.0.0
lib/libjpeg.so
lib/libxml2.so.2
lib/libgd.so.2
php
php/php.ini
phpinfo.php
root@Moxa:/mnt/ramdisk#
```

Step 5: Run 'install.sh' and select to install php

```

192.168.3.127 - PuTTY
root@Moxa:/mnt/ramdisk# ./install.sh
Press the number:
1. Install PHP package
2. Uninstall PHP package
3. Exit.
1
Start to install PHP. Please wait ...
Starting web server: apache.
PHP install success.
root@Moxa:/mnt/ramdisk#

```

Step 6: Test it. Use the browser to access <http://192.168.3.127/phpinfo.php>

The screenshot shows a Microsoft Internet Explorer browser window displaying the PHP Version 5.0.5 information page. The page title is 'phpinfo() - Microsoft Internet Explorer'. The address bar shows 'http://192.168.27.139/phpinfo.php'. The main content area displays the following information:

PHP Version 5.0.5

| | |
|-------------------------------------|---|
| System | Linux Moxa 2.6.9-uc0 #1048 Tue May 9 15:56:02 CST 2006 armv4tl |
| Build Date | Apr 4 2006 22:12:06 |
| Configure Command | ./configure '--build=i686-linux' '--host=arm-linux' '--target=arm-linux' '--with-apxs2=/home/victor/ia-240-241/source_code/user/apache/install_me/bin/apxs' '--with-zlib' '--with-gettext' '--disable-cg' '--enable-force-cv-redirect' '--prefix=/home/victor/ia-240-241/source_code/user/php/install_me' '--with-openssl' '--with-mysql=/home/victor/ia-240-241/source_code/user/mysql/install_me' '--with-config-file-path=/etc/apache/php' '--with-gd=/home/victor/ia-240-241/source_code/lib/libgd/install_me' '--with-libxml-dir=/home/victor/ia-240-241/source_code/lib/libxml2/install_me' |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/apache/php/php.ini |
| PHP API | 20031224 |
| PHP Extension | 20041030 |
| Zend Extension | 220040412 |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Memory Manager | enabled |
| IPv6 Support | enabled |
| Registered PHP Streams | php, file, http, ftp, compress.zlib, https, ftps |
| Registered Stream Socket Transports | tcp, udp, unix, udg, ssl, sslv3, sslv2, tls |

This program makes use of the Zend Scripting Language Engine:
 Zend Engine v2.0.5, Copyright (c) 1998-2004 Zend Technologies

Powered By

PHP Credits

If you want to uninstall PHP, follow steps 2 to 5 but select the uninstall option.

IPTABLES

IPTABLES is an administrative tool for setting up, maintaining, and inspecting the Linux kernel's IP packet filter rule tables. Several different tables are defined, with each table containing built-in chains and user-defined chains.

Each chain is a list of rules that apply to a certain type of packet. Each rule specifies what to do with a matching packet. A rule (such as a jump to a user-defined chain in the same table) is called a "target."

The W311/321/341 support 3 types of IPTABLES table: **Filter** tables, **NAT** tables, and **Mangle** tables:

A. **Filter Table**—includes three chains:

- INPUT chain
- OUTPUT chain
- FORWARD chain

B. **NAT Table**—includes three chains:

- PREROUTING chain—transfers the destination IP address (DNAT)

- POSTROUTING chain—works after the routing process and before the Ethernet device process to transfer the source IP address (SNAT)

- OUTPUT chain—produces local packets

sub-tables

- Source NAT (SNAT)—changes the first source packet IP address

- Destination NAT (DNAT)—changes the first destination packet IP address

- MASQUERADE—a special form for SNAT. If one host can connect to Internet, then other computers that connect to this host can connect to the Internet when the computer does not have an actual IP address.

- REDIRECT—a special form of DNAT that re-sends packets to a local host independent of the destination IP address.

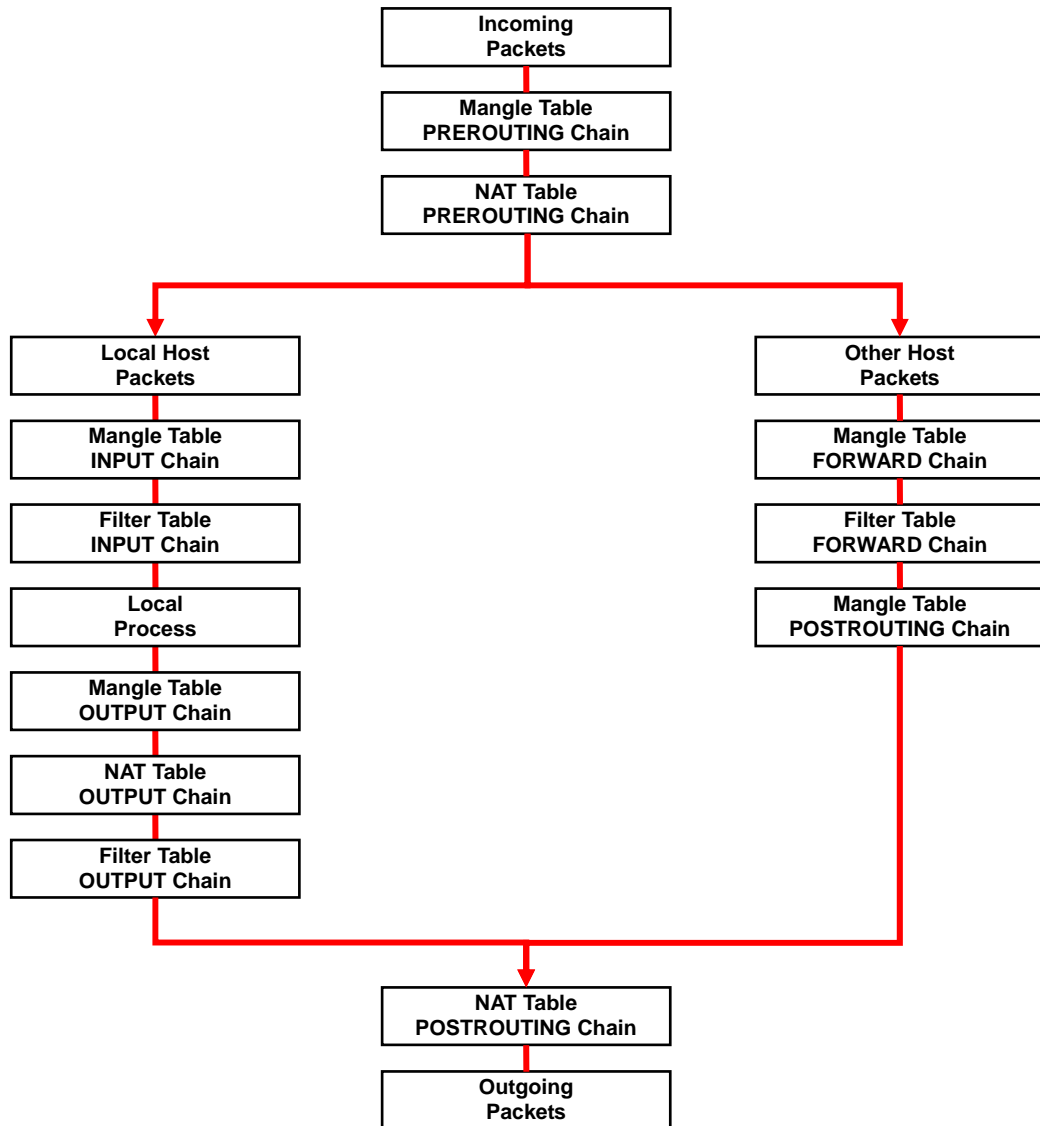
C. **Mangle Table**—includes two chains

- PREROUTING chain—pre-processes packets before the routing process.

- OUTPUT chain—processes packets after the routing process.

It has three extensions—TTL, MARK, TOS.

The following figure shows the IPTABLES hierarchy.



The W311/321/341 support the following sub-modules. Be sure to use the module that matches your application.

| | | | |
|-------------------|----------------|---------------|-------------|
| ip_conntrack | ipt_MARK | ipt_ah | ipt_state |
| ip_conntrack_ftp | ipt_MASQUERADE | ipt_esp | ipt_tcpmss |
| ipt_conntrack_irc | ipt_MIRROT | ipt_length | ipt_tos |
| ip_nat_ftp | ipt_REDIRECT | ipt_limit | ipt_ttl |
| ip_nat_irc | ipt_REJECT | ipt_mac | ipt_unclean |
| ip_nat_snmp_basic | ipt_TCPMSS | ipt_mark | |
| ip_queue | ipt_TOS | ipt_multiport | |
| ipt_LOG | ipt_ULOG | ipt_owner | |

NOTE The W311/321/341 do NOT support IPV6 and ipchains.

The basic syntax to enable and load an IPTABLES module is as follows:

```
#lsmod
#insmod ip_tables
#insmod iptable_filter
```

Use `lsmod` to check if the `ip_tables` module has already been loaded in the W311/321/341 unit. Use `insmod` to insert and enable the module.

Use the following command to load the modules (`iptable_filter`, `iptable_mangle`, `iptable_nat`):

```
#insmod iptable_filter
```

Use `iptables`, `iptables-restore`, `iptables-save` to maintain the database.

NOTE IPTABLES plays the role of packet filtering or NAT. Take care when setting up the IPTABLES rules. If the rules are not correct, remote hosts that connect via a LAN or PPP may be denied access. We recommend using the serial console to set up the IPTABLES.

Click on the following links for more information about iptables.

<http://www.linuxguruz.com/iptables/>

<http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO.html>

Since the IPTABLES command is very complex, to illustrate the IPTABLES syntax we have divided our discussion of the various rules into three categories: **Observe and erase chain rules**, **Define policy rules**, and **Append or delete rules**.

Observe and erase chain rules

Usage:

```
# iptables [-t tables] [-L] [-n]
  -t tables:  Table to manipulate (default: 'filter'); example: nat or filter.
  -L [chain]: List all rules in selected chains. If no chain is selected, all chains are listed.
  -n:        Numeric output of addresses and ports.

# iptables [-t tables] [-FXZ]
  -F: Flush the selected chain (all the chains in the table if none is listed).
  -X: Delete the specified user-defined chain.
  -Z: Set the packet and byte counters in all chains to zero.
```

Examples:

```
# iptables -L -n
```

In this example, since we do not use the `-t` parameter, the system uses the default 'filter' table. Three chains are included: INPUT, OUTPUT, and FORWARD. INPUT chains are accepted automatically, and all connections are accepted without being filtered.

```
#iptables -F
#iptables -X
#iptables -Z
```

Define policy for chain rules

Usage:

```
# iptables [-t tables] [-P] [INPUT, OUTPUT, FORWARD, PREROUTING, OUTPUT, POSTROUTING]
[ACCEPT, DROP]
-P:      Set the policy for the chain to the given target.
INPUT:   For packets coming into the W311/321/341.
OUTPUT:  For locally-generated packets.
FORWARD: For packets routed out through the W311/321/341.
PREROUTING: To alter packets as soon as they come in.
POSTROUTING: To alter packets as they are about to be sent out.
```

Examples:

```
#iptables -P INPUT DROP
#iptables -P OUTPUT ACCEPT
#iptables -P FORWARD ACCEPT
#iptables -t nat -P PREROUTING ACCEPT
#iptables -t nat -P OUTPUT ACCEPT
#iptables -t nat -P POSTROUTING ACCEPT
```

In this example, the policy accepts outgoing packets and denies incoming packets.

Append or delete rules:

Usage:

```
# iptables [-t table] [-AI] [INPUT, OUTPUT, FORWARD] [-io interface] [-p tcp, udp, icmp,
all] [-s IP/network] [--sport ports] [-d IP/network] [--dport ports] -j [ACCEPT, DROP]
-A:      Append one or more rules to the end of the selected chain.
-I:      Insert one or more rules in the selected chain as the given rule number.
-i:      Name of an interface via which a packet is going to be received.
-o:      Name of an interface via which a packet is going to be sent.
-p:      The protocol of the rule or of the packet to check.
-s:      Source address (network name, host name, network IP address, or plain IP address).
--sport: Source port number.
-d:      Destination address.
--dport: Destination port number.
-j:      Jump target. Specifies the target of the rules; i.e., how to handle matched packets. For
example, ACCEPT the packet, DROP the packet, or LOG the packet.
```

Examples:

Example 1: Accept all packets from lo interface.

```
# iptables -A INPUT -i lo -j ACCEPT
```

Example 2: Accept TCP packets from 192.168.0.1.

```
# iptables -A INPUT -i eth0 -p tcp -s 192.168.0.1 -j ACCEPT
```

Example 3: Accept TCP packets from Class C network 192.168.1.0/24.

```
# iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 -j ACCEPT
```

Example 4: Drop TCP packets from 192.168.1.25.

```
# iptables -A INPUT -i eth0 -p tcp -s 192.168.1.25 -j DROP
```

Example 5: Drop TCP packets addressed for port 21.

```
# iptables -A INPUT -i eth0 -p tcp --dport 21 -j DROP
```

Example 6: Accept TCP packets from 192.168.0.24 to W341's port 137, 138, 139

```
# iptables -A INPUT -i eth0 -p tcp -s 192.168.0.24 --dport 137:139 -j ACCEPT
```

Example 8: Drop all packets from MAC address 01:02:03:04:05:06.

```
# iptables -A INPUT -i eth0 -p all -m mac --mac-source 01:02:03:04:05:06 -j DROP
```

NOTE: In Example 8, remember to issue the command `#insmod ipt_mac` first to load module `ipt_mac`.

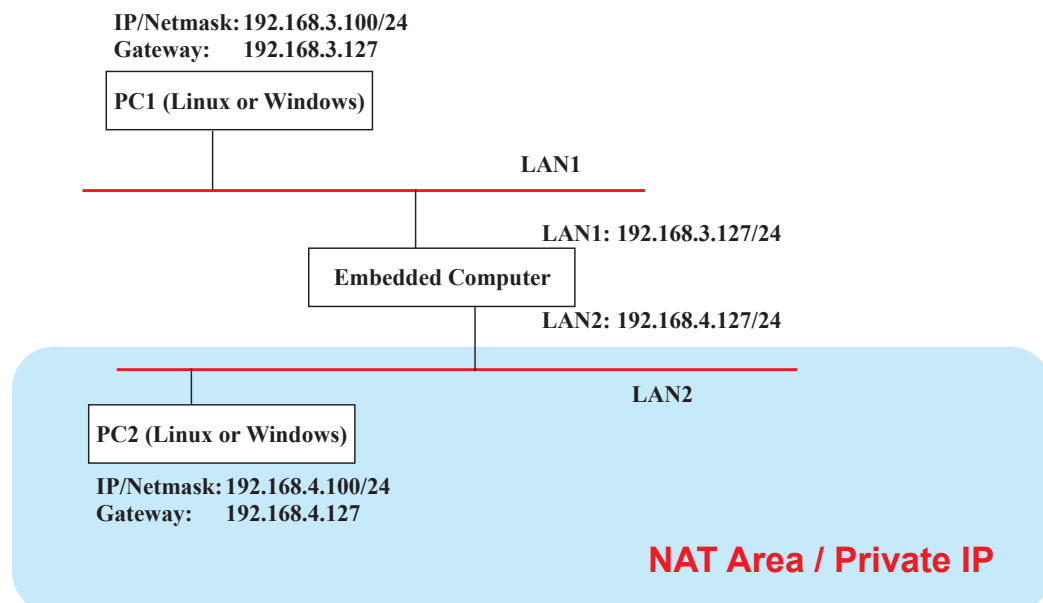
NAT

NAT (Network Address Translation) protocol translates IP addresses used on one network to different IP addresses used on another network. One network is designated the inside network and the other is the outside network. Typically, the W311/321/341 connect several devices on a network and maps local inside network addresses to one or more global outside IP addresses, and un-maps the global IP addresses on incoming packets back into local IP addresses.

NOTE Click on the following link for more information about iptables and NAT:
<http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html>

NAT Example

The IP address of LAN1 is changed to 192.168.3.127 (you will need to load the module `ipt_MASQUERADE`):



1. `#echo 1 > /proc/sys/net/ipv4/ip_forward`
2. `#insmod ip_tables`
3. `#insmod iptable_filter`
4. `#insmod ip_conntrack`
5. `#insmod iptable_nat`
6. `#insmod ipt_MASQUERADE`
7. `#iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.3.127`
8. `#iptables -t nat -A POSTROUTING -o eth0 -s 192.168.3.0/24 -j MASQUERADE`

Enabling NAT at Bootup

In most real world situations, you will want to use a simple shell script to enable NAT when the W341 boots up. The following script is an example.

```
#!/bin/bash
# If you put this shell script in the /home/nat.sh
# Remember to chmod 744 /home/nat.sh
# Edit the rc.local file to make this shell startup automatically.
# vi /etc/rc.d/rc.local
# Add a line in the end of rc.local /home/nat.sh
EXIF='eth0' #This is an external interface for setting up a valid IP address.
EXNET='192.168.4.0/24' #This is an internal network address.
# Step 1. Insert modules.
# Here 2> /dev/null means the standard error messages will be dump to null device.
insmod ip_tables 2> /dev/null
insmod ip_conntrack 2> /dev/null
insmod ip_conntrack_ftp 2> /dev/null
insmod ip_conntrack_irc 2> /dev/null
insmod iptable_nat 2> /dev/null
insmod ip_nat_ftp 2> /dev/null
insmod ip_nat_irc 2> /dev/null
# Step 2. Define variables, enable routing and erase default rules.
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
export PATH
echo "1" > /proc/sys/net/ipv4/ip_forward
/bin/iptables -F
/bin/iptables -X
/bin/iptables -Z
/bin/iptables -F -t nat
/bin/iptables -X -t nat
/bin/iptables -Z -t nat
/bin/iptables -P INPUT ACCEPT
/bin/iptables -P OUTPUT ACCEPT
/bin/iptables -P FORWARD ACCEPT
/bin/iptables -t nat -P PREROUTING ACCEPT
/bin/iptables -t nat -P POSTROUTING ACCEPT
/bin/iptables -t nat -P OUTPUT ACCEPT
# Step 3. Enable IP masquerade.
```

Dial-up Service—PPP

PPP (Point to Point Protocol) is used to run IP (Internet Protocol) and other network protocols over a serial link. PPP can be used for direct serial connections (using a null-modem cable) over a Telnet link, and links established using a modem over a telephone line.

Modem / PPP access is almost identical to connecting directly to a network through the W311/321/341's Ethernet port. Since PPP is a peer-to-peer system, the W311/321/341 can also use PPP to link two networks (or a local network to the Internet) to create a Wide Area Network (WAN).

NOTE Click on the following links for more information about ppp:
<http://tldp.org/HOWTO/PPP-HOWTO/index.html>
<http://axion.physics.ubc.ca/ppp-linux.html>

The pppd daemon is used to connect to a PPP server from a Linux system. For detailed information about pppd see the man page.

Example 1: Connecting to a PPP server over a simple dial-up connection

The following command is used to connect to a PPP server by modem. Use this command for old ppp servers that prompt for a login name (replace *username* with the correct name) and password (replace *password* with the correct password). Note that *debug* and *defaultroute 192.1.1.17* are

optional.

```
#pppd connect `chat -v ` ` ATDT5551212 CONNECT ` ` ogin: username word: password`
/dev/ttyM0 115200 debug crtscts modem defaultroute
```

If the PPP server does not prompt for the username and password, the command should be entered as follows. Replace *username* with the correct username and replace *password* with the correct password.

```
#pppd connect `chat -v ` ` ATDT5551212 CONNECT ` ` `user username password password`
/dev/ttyM0 115200 crtscts modem
```

The pppd options are described below:

connect *`chat etc...`*

This option gives the command to contact the PPP server. The 'chat' program is used to dial a remote computer. The entire command is enclosed in single quotes because pppd expects a one-word argument for the 'connect' option. The options for 'chat' are given below:

-v

verbose mode; log what we do to syslog

` `

Double quotes—don't wait for a prompt, but instead do ... (note that you must include a space after the second quotation mark)

ATDT5551212

Dial the modem, and then ...

CONNECT

Wait for an answer.

` `

Send a return (null text followed by the usual return)

ogin: *username* word: *password*

Log in with *username* and *password*.

Refer to the chat man page, chat.8, for more information about the chat utility.

/dev/

Specify the callout serial port.

115200

The baudrate.

debug

Log status in syslog.

crtscts

Use hardware flow control between computer and modem (at 115200 this is a must).

modem

Indicates that this is a modem device; pppd will hang up the phone before and after making the call.

defaultroute

Once the PPP link is established, make it the default route; if you have a PPP link to the Internet, this is probably what you want.

192.1.1.17

This is a degenerate case of a general option of the form *x.x.x.x:y.y.y.y*. Here *x.x.x.x* is the local IP address and *y.y.y.y* is the IP address of the remote end of the PPP connection. If this option is not specified, or if just one side is specified, then *x.x.x.x* defaults to the IP address associated with the local machine's hostname (located in **/etc/hosts**), and *y.y.y.y* is determined by the remote machine.

Example 2: Connecting to a PPP server over a hard-wired link

If a username and password are not required, use the following command (note that *noipdefault* is optional):

```
#pppd connect `chat -v " " " " ` noipdefault /dev/ttyM0 19200 crtscts
```

If a username and password is required, use the following command (note that *noipdefault* is optional, and *root* is both the username and password):

```
#pppd connect `chat -v " " " " ` user root password root noipdefault /dev/ttyM0 19200 crtscts
```

How to check the connection

Once you've set up a PPP connection, there are some steps you can take to test the connection.

First, type:

```
/sbin/ifconfig
```

(The folder **ifconfig** may be located elsewhere, depending on your distribution.) You should be able to see all the network interfaces that are UP. `ppp0` should be one of them, and you should recognize the first IP address as your own, and the "P-t-P address" (or point-to-point address) the address of your server. Here's what it looks like on one machine:

```
lo      Link encap Local Loopback
        inet addr 127.0.0.1  Bcast 127.255.255.255  Mask 255.0.0.0
        UP LOOPBACK RUNNING  MTU 2000  Metric 1
        RX packets 0 errors 0 dropped 0 overrun 0

ppp0    Link encap Point-to-Point Protocol
        inet addr 192.76.32.3  P-t-P 129.67.1.165  Mask 255.255.255.0
        UP POINTOPOINT RUNNING  MTU 1500  Metric 1
        RX packets 33 errors 0 dropped 0 overrun 0
        TX packets 42 errors 0 dropped 0 overrun 0
```

Now, type:

```
ping z.z.z.z
```

where `z.z.z.z` is the address of your name server. This should work. Here's what the response could look like:

```
waddington:~$ping 129.67.1.165
PING 129.67.1.165 (129.67.1.165): 56 data bytes
64 bytes from 129.67.1.165: icmp_seq=0 ttl=225 time=268 ms
64 bytes from 129.67.1.165: icmp_seq=1 ttl=225 time=247 ms
64 bytes from 129.67.1.165: icmp_seq=2 ttl=225 time=266 ms
^C
--- 129.67.1.165 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 247/260/268 ms
waddington:~$
```

Try typing:

```
netstat -nr
```

This should show three routes, something like this:

```
Kernel routing table
Destination      Gateway          Genmask          Flags      Metric    Ref    Use
iface
129.67.1.165     0.0.0.0          255.255.255.255 UH         0         0      6
ppp0
127.0.0.0        0.0.0.0          255.0.0.0       U          0         0      0 lo
0.0.0.0          129.67.1.165    0.0.0.0         UG         0         0     6298
ppp0
```

If your output looks similar but doesn't have the destination 0.0.0.0 line (which refers to the default route used for connections), you may have run `pppd` without the `'defaultroute'` option. At this point you can try using Telnet, ftp, or finger, bearing in mind that you'll have to use numeric IP addresses unless you've set up `/etc/resolv.conf` correctly.

Setting up a Machine for Incoming PPP Connections

This first example applies to using a modem, and requiring authorization with a username and password.

```
pppd/dev/ttyM0 115200 crtscts modem 192.168.16.1:192.168.16.2 login auth
```

You should also add the following line to the file `/etc/ppp/pap-secrets`:

```
* * "" *
```

The first star (*) lets everyone login. The second star (*) lets every host connect. The pair of double quotation marks ("") is to use the file `/etc/passwd` to check the password. The last star (*) is to let any IP connect.

The following example does not check the username and password:

```
pppd/dev/ttyM0 115200 crtscts modem 192.168.16.1:192.168.16.2
```

PPPoE

1. Connect the W311/321/341's LAN port to an ADSL modem with a cross-over cable, HUB, or switch.
2. Log in to the W311/321/341 as the root user.
3. Edit the file `/etc/ppp/chap-secrets` and add the following:
"username@hinet.net"*"password"*

```
# Secrets for authentication using CHAP
# client      server      secret      IP addresses
"username@hinet.net" * "password" *
:
:
:
"chap-secrets" line 1 of 3 --33%--
```

"username@hinet.net" is the username obtained from the ISP to log in to the ISP account.
"password" is the corresponding password for the account.

4. Edit the file `/etc/ppp/pap-secrets` and add the following:

`"username@hinet.net"*"password"*`

```
# password if you don't use the login option of pppd! The mgetty Debian
# package already provides this option; make sure you don't change that.

# INBOUND connections
~
# Every regular user can use PPP and has to use passwords from /etc/passwd
"username@hinet.net" * "password" *
~
# UserIDs that cannot use PPP at all. Check your /etc/passwd and add any
# other accounts that should not be able to use pppd!
guest hostname "*" -
master hostname "*" -
root hostname "*" -
support hostname "*" -
stats hostname "*" -

# OUTBOUND connections

# Here you should add your userid password to connect to your providers via
# PAP. The * means that the password is to be used for ANY host you connect
# to. Thus you do not have to worry about the foreign machine name. Just
# replace password with your password.
"pap-secrets" line 1 of 42 --2%--
```

`"username@hinet.net"` is the username obtained from the ISP to log in to the ISP account.
`"password"` is the corresponding password for the account.

5. Edit the file `/etc/ppp/options` and add the following line:

`plugin pppoe`

```
# terminated because it was idle.
#holdoff <n>

# Wait for up n milliseconds after the connect script finishes for a valid
# PPP packet from the peer. At the end of this time, or when a valid PPP
# packet is received from the peer, pppd will commence negotiation by
# sending its first LCP packet. The default value is 1000 (1 second).
# This wait period only applies if the connect or pty option is used.
#connect delay <n>
plugin pppoe.so
~
# ---<End of File>---
~
~
~
~
~
~
~
~
~
~
"options" line 1 of 342 --0%--
```


NOTE Click on the following links for more information about NFS:

<http://www.tldp.org/HOWTO/NFS-HOWTO/index.html>

<http://nfs.sourceforge.net/nfs-howto/client.html>

<http://nfs.sourceforge.net/nfs-howto/server.html>

Setting up the W311/321/341 as an NFS Client

The following procedure is used to mount a remote NFS Server.

1. To know the NFS Server's shared directory.
2. Establish a mount point on the NFS Client site.
3. Mount the remote directory to a local directory.

```
#mkdir -p /home/nfs/public
#mount -t nfs NFS_Server(IP):/directory /mount/point
```

Example

```
#mount -t nfs 192.168.3.100:/home/public /home/nfs/public
```

Mail

smtpclient is a minimal SMTP client that takes an email message body and passes it on to an SMTP server. It is suitable for applications that use email to send alert messages or important logs to a specific user.

NOTE Click on the following link for more information about smtpclient:

<http://www.engelschall.com/sw/smtpclient/>

To send an email message, use the 'smtpclient' utility, which uses SMTP protocol. Type

```
#smtpclient -help to see the help message.
```

Example:

```
smtpclient -s test -f sender@company.com -S IP_address receiver@company.com
< mail-body-message
```

- s: The mail subject.
- f: Sender's mail address
- S: SMTP server IP address

The last mail address **receiver@company.com** is the receiver's e-mail address.

mail-body-message is the mail content. The last line of the body of the message should contain ONLY the period '.' character.

You will need to add your hostname to the file **/etc/hosts**.

SNMP

The W311/321/341 have built-in SNMP V1 (Simple Network Management Protocol) agent software. It supports RFC1317 RS-232 like group and RFC 1213 MIB-II.

The following simple example allows you to use an SNMP browser on the host site to query the W311/321/341, which is the SNMP agent. The W311/321/341 will respond.

```
***** SNMP QUERY STARTED *****
```

```
1: sysDescr.0 (octet string) Version 1.0
```

```
2: sysObjectID.0 (object identifier) enterprises.8691.12.240
```

3: sysUpTime.0 (timeticks) 0 days 03h:50m:11s.00th (1381100)
4: sysContact.0 (octet string) Moxa Systems Co., LDT.
5: sysName.0 (octet string) Moxa
6: sysLocation.0 (octet string) Unknown
7: sysServices.0 (integer) 6
8: ifNumber.0 (integer) 6
9: ifIndex.1 (integer) 1
10: ifIndex.2 (integer) 2
11: ifIndex.3 (integer) 3
12: ifIndex.4 (integer) 4
13: ifIndex.5 (integer) 5
14: ifIndex.6 (integer) 6
15: ifDescr.1 (octet string) eth0
16: ifDescr.2 (octet string) eth1
17: ifDescr.3 (octet string) Serial port 0
18: ifDescr.4 (octet string) Serial port 1
19: ifDescr.5 (octet string) Serial port 2
20: ifDescr.6 (octet string) Serial port 3
21: ifType.1 (integer) ethernet-csmacd(6)
22: ifType.2 (integer) ethernet-csmacd(6)
23: ifType.3 (integer) other(1)
24: ifType.4 (integer) other(1)
25: ifType.5 (integer) other(1)
26: ifType.6 (integer) other(1)
27: ifMtu.1 (integer) 1500
28: ifMtu.2 (integer) 1500
29: ifMtu.3 (integer) 0
30: ifMtu.4 (integer) 0
31: ifMtu.5 (integer) 0
32: ifMtu.6 (integer) 0
33: ifSpeed.1 (gauge) 100000000
34: ifSpeed.2 (gauge) 100000000
35: ifSpeed.3 (gauge) 38400
36: ifSpeed.4 (gauge) 38400
37: ifSpeed.5 (gauge) 38400
38: ifSpeed.6 (gauge) 38400
39: ifPhysAddress.1 (octet string) 00.90.E8.10.02.41 (hex)
40: ifPhysAddress.2 (octet string) 00.90.E8.10.02.40 (hex)
41: ifPhysAddress.3 (octet string) 00 (hex)
42: ifPhysAddress.4 (octet string) 00 (hex)
43: ifPhysAddress.5 (octet string) 00 (hex)
44: ifPhysAddress.6 (octet string) 00 (hex)
45: ifAdminStatus.1 (integer) up(1)
46: ifAdminStatus.2 (integer) up(1)
47: ifAdminStatus.3 (integer) down(2)
48: ifAdminStatus.4 (integer) down(2)
49: ifAdminStatus.5 (integer) down(2)
50: ifAdminStatus.6 (integer) down(2)
51: ifOperStatus.1 (integer) up(1)
52: ifOperStatus.2 (integer) up(1)
53: ifOperStatus.3 (integer) down(2)
54: ifOperStatus.4 (integer) down(2)
55: ifOperStatus.5 (integer) down(2)
56: ifOperStatus.6 (integer) down(2)
57: ifLastChange.1 (timeticks) 0 days 00h:00m:00s.00th (0)
58: ifLastChange.2 (timeticks) 0 days 00h:00m:00s.00th (0)
59: ifLastChange.3 (timeticks) 0 days 00h:00m:00s.00th (0)
60: ifLastChange.4 (timeticks) 0 days 00h:00m:00s.00th (0)
61: ifLastChange.5 (timeticks) 0 days 00h:00m:00s.00th (0)
62: ifLastChange.6 (timeticks) 0 days 00h:00m:00s.00th (0)
63: ifInOctets.1 (counter) 25511
64: ifInOctets.2 (counter) 2240203
65: ifInOctets.3 (counter) 0
66: ifInOctets.4 (counter) 0
67: ifInOctets.5 (counter) 0
68: ifInOctets.6 (counter) 0
69: ifInUcastPkts.1 (counter) 254

70: ifInUcastPkts.2 (counter) 28224
71: ifInUcastPkts.3 (counter) 0
72: ifInUcastPkts.4 (counter) 0
73: ifInUcastPkts.5 (counter) 0
74: ifInUcastPkts.6 (counter) 0
75: ifInNUcastPkts.1 (counter) 0
76: ifInNUcastPkts.2 (counter) 0
77: ifInNUcastPkts.3 (counter) 0
78: ifInNUcastPkts.4 (counter) 0
79: ifInNUcastPkts.5 (counter) 0
80: ifInNUcastPkts.6 (counter) 0
81: ifInDiscards.1 (counter) 0
82: ifInDiscards.2 (counter) 0
83: ifInDiscards.3 (counter) 0
84: ifInDiscards.4 (counter) 0
85: ifInDiscards.5 (counter) 0
86: ifInDiscards.6 (counter) 0
87: ifInErrors.1 (counter) 0
88: ifInErrors.2 (counter) 0
89: ifInErrors.3 (counter) 0
90: ifInErrors.4 (counter) 0
91: ifInErrors.5 (counter) 0
92: ifInErrors.6 (counter) 0
93: ifInUnknownProtos.1 (counter) 0
94: ifInUnknownProtos.2 (counter) 0
95: ifInUnknownProtos.3 (counter) 0
96: ifInUnknownProtos.4 (counter) 0
97: ifInUnknownProtos.5 (counter) 0
98: ifInUnknownProtos.6 (counter) 0
99: ifOutOctets.1 (counter) 51987
100: ifOutOctets.2 (counter) 3832
101: ifOutOctets.3 (counter) 0
102: ifOutOctets.4 (counter) 0
103: ifOutOctets.5 (counter) 0
104: ifOutOctets.6 (counter) 0
105: ifOutUcastPkts.1 (counter) 506
106: ifOutUcastPkts.2 (counter) 42
107: ifOutUcastPkts.3 (counter) 0
108: ifOutUcastPkts.4 (counter) 0
109: ifOutUcastPkts.5 (counter) 0
110: ifOutUcastPkts.6 (counter) 0
111: ifOutNUcastPkts.1 (counter) 0
112: ifOutNUcastPkts.2 (counter) 0
113: ifOutNUcastPkts.3 (counter) 0
114: ifOutNUcastPkts.4 (counter) 0
115: ifOutNUcastPkts.5 (counter) 0
116: ifOutNUcastPkts.6 (counter) 0
117: ifOutDiscards.1 (counter) 0
118: ifOutDiscards.2 (counter) 0
119: ifOutDiscards.3 (counter) 0
120: ifOutDiscards.4 (counter) 0
121: ifOutDiscards.5 (counter) 0
122: ifOutDiscards.6 (counter) 0
123: ifOutErrors.1 (counter) 0
124: ifOutErrors.2 (counter) 0
125: ifOutErrors.3 (counter) 0
126: ifOutErrors.4 (counter) 0
127: ifOutErrors.5 (counter) 0
128: ifOutErrors.6 (counter) 0
129: ifOutQLen.1 (gauge) 1000
130: ifOutQLen.2 (gauge) 1000
131: ifOutQLen.3 (gauge) 0
132: ifOutQLen.4 (gauge) 0
133: ifOutQLen.5 (gauge) 0
134: ifOutQLen.6 (gauge) 0
135: ifSpecific.1 (object identifier) (null-oid) zeroDotZero
136: ifSpecific.2 (object identifier) (null-oid) zeroDotZero

137: ifSpecific.3 (object identifier) (null-oid) zeroDotZero
138: ifSpecific.4 (object identifier) (null-oid) zeroDotZero
139: ifSpecific.5 (object identifier) (null-oid) zeroDotZero
140: ifSpecific.6 (object identifier) (null-oid) zeroDotZero
141: atIfIndex.1.192.168.27.139 (integer) 1
142: atIfIndex.2.192.168.4.127 (integer) 2
143: atPhysAddress.1.192.168.27.139 (octet string) 00.90.E8.10.02.41 (hex)
144: atPhysAddress.2.192.168.4.127 (octet string) 00.90.E8.10.02.40 (hex)
145: atNetAddress.1.192.168.27.139 (ipaddress) 192.168.27.139
146: atNetAddress.2.192.168.4.127 (ipaddress) 192.168.4.127
147: ipForwarding.0 (integer) forwarding(1)
148: ipDefaultTTL.0 (integer) 64
149: ipInReceives.0 (counter) 1289
150: ipInHdrErrors.0 (counter) 0
151: ipInAddrErrors.0 (counter) 0
152: ipForwDatagrams.0 (counter) 9
153: ipInUnknownProtos.0 (counter) 0
154: ipInDiscards.0 (counter) 0
155: ipInDelivers.0 (counter) 1160
156: ipOutRequests.0 (counter) 858
157: ipOutDiscards.0 (counter) 0
158: ipOutNoRoutes.0 (counter) 0
159: ipReasmTimeout.0 (integer) 0
160: ipReasmReqs.0 (counter) 0
161: ipReasmOKs.0 (counter) 0
162: ipReasmFails.0 (counter) 0
163: ipFragOKs.0 (counter) 0
164: ipFragFails.0 (counter) 0
165: ipFragCreates.0 (counter) 0
166: ipAdEntAddr.192.168.27.139 (ipaddress) 192.168.27.139
167: ipAdEntAddr.192.168.4.127 (ipaddress) 192.168.4.127
168: ipAdEntIfIndex.192.168.27.139 (integer) 1
169: ipAdEntIfIndex.192.168.4.127 (integer) 2
170: ipAdEntNetMask.192.168.27.139 (ipaddress) 255.255.255.0
171: ipAdEntNetMask.192.168.4.127 (ipaddress) 255.255.255.0
172: ipAdEntBcastAddr.192.168.27.139 (integer) 1
173: ipAdEntBcastAddr.192.168.4.127 (integer) 1
174: ipAdEntReasmMaxSize.192.168.27.139 (integer) 65535
175: ipAdEntReasmMaxSize.192.168.4.127 (integer) 65535
176: ipRouteDest.192.168.4.0 (ipaddress) 192.168.4.0
177: ipRouteDest.192.168.27.0 (ipaddress) 192.168.27.0
178: ipRouteIfIndex.192.168.4.0 (integer) 2
179: ipRouteIfIndex.192.168.27.0 (integer) 1
180: ipRouteMetric1.192.168.4.0 (integer) 0
181: ipRouteMetric1.192.168.27.0 (integer) 0
182: ipRouteMetric2.192.168.4.0 (integer) -1
183: ipRouteMetric2.192.168.27.0 (integer) -1
184: ipRouteMetric3.192.168.4.0 (integer) -1
185: ipRouteMetric3.192.168.27.0 (integer) -1
186: ipRouteMetric4.192.168.4.0 (integer) -1
187: ipRouteMetric4.192.168.27.0 (integer) -1
188: ipRouteNextHop.192.168.4.0 (ipaddress) 192.168.4.127
189: ipRouteNextHop.192.168.27.0 (ipaddress) 192.168.27.139
190: ipRouteType.192.168.4.0 (integer) direct(3)
191: ipRouteType.192.168.27.0 (integer) direct(3)
192: ipRouteProto.192.168.4.0 (integer) local(2)
193: ipRouteProto.192.168.27.0 (integer) local(2)
194: ipRouteAge.192.168.4.0 (integer) 0
195: ipRouteAge.192.168.27.0 (integer) 0
196: ipRouteMask.192.168.4.0 (ipaddress) 255.255.255.0
197: ipRouteMask.192.168.27.0 (ipaddress) 255.255.255.0
198: ipRouteMetric5.192.168.4.0 (integer) -1
199: ipRouteMetric5.192.168.27.0 (integer) -1
200: ipRouteInfo.192.168.4.0 (object identifier) (null-oid) zeroDotZero
201: ipRouteInfo.192.168.27.0 (object identifier) (null-oid) zeroDotZero
202: ipNetToMediaIfIndex.1.192.168.27.139 (integer) 1
203: ipNetToMediaIfIndex.2.192.168.4.127 (integer) 2

204: ipNetToMediaPhysAddress.1.192.168.27.139 (octet string) 00.90.E8.10.02.41 (hex)
 205: ipNetToMediaPhysAddress.2.192.168.4.127 (octet string) 00.90.E8.10.02.40 (hex)
 206: ipNetToMediaNetAddress.1.192.168.27.139 (ipaddress) 192.168.27.139
 207: ipNetToMediaNetAddress.2.192.168.4.127 (ipaddress) 192.168.4.127
 208: ipNetToMediaType.1.192.168.27.139 (integer) static(4)
 209: ipNetToMediaType.2.192.168.4.127 (integer) static(4)
 210: ipRoutingDiscards.0 (integer) 0
 211: icmpInMsgs.0 (counter) 130
 212: icmpInErrors.0 (counter) 3
 213: icmpInDestUnreachs.0 (counter) 128
 214: icmpInTimeExcds.0 (counter) 0
 215: icmpInParmProbs.0 (counter) 0
 216: icmpInSrcQuenchs.0 (counter) 0
 217: icmpInRedirects.0 (counter) 0
 218: icmpInEchos.0 (counter) 2
 219: icmpInEchoReps.0 (counter) 0
 220: icmpInTimestamps.0 (counter) 0
 221: icmpInTimestampReps.0 (counter) 0
 222: icmpInAddrMasks.0 (counter) 0
 223: icmpInAddrMaskReps.0 (counter) 0
 224: icmpOutMsgs.0 (counter) 144
 225: icmpOutErrors.0 (counter) 0
 226: icmpOutDestUnreachs.0 (counter) 135
 227: icmpOutTimeExcds.0 (counter) 0
 228: icmpOutParmProbs.0 (counter) 0
 229: icmpOutSrcQuenchs.0 (counter) 0
 230: icmpOutRedirects.0 (counter) 7
 231: icmpOutEchos.0 (counter) 0
 232: icmpOutEchoReps.0 (counter) 2
 233: icmpOutTimestamps.0 (counter) 0
 234: icmpOutTimestampReps.0 (counter) 0
 235: icmpOutAddrMasks.0 (counter) 0
 236: icmpOutAddrMaskReps.0 (counter) 0
 237: tcpRtoAlgorithm.0 (integer) other(1)
 238: tcpRtoMin.0 (integer) 200
 239: tcpRtoMax.0 (integer) 120000
 240: tcpMaxConn.0 (integer) -1
 241: tcpActiveOpens.0 (counter) 0
 242: tcpPassiveOpens.0 (counter) 0
 243: tcpAttemptFails.0 (counter) 0
 244: tcpEstabResets.0 (counter) 0
 245: tcpCurrEstab.0 (gauge) 0
 246: tcpInSegs.0 (counter) 0
 247: tcpOutSegs.0 (counter) 0
 248: tcpRetransSegs.0 (counter) 0
 249: tcpConnState.192.168.27.139.1024.0.0.0.0.0 (integer) listen(2)
 250: tcpConnState.192.168.4.127.1024.0.0.0.0.0 (integer) listen(2)
 251: tcpConnState.192.168.27.139.1025.0.0.0.0.0 (integer) listen(2)
 252: tcpConnState.192.168.4.127.1025.0.0.0.0.0 (integer) listen(2)
 253: tcpConnState.192.168.27.139.2049.0.0.0.0.0 (integer) listen(2)
 254: tcpConnState.192.168.4.127.2049.0.0.0.0.0 (integer) listen(2)
 255: tcpConnState.192.168.27.139.1026.0.0.0.0.0 (integer) listen(2)
 256: tcpConnState.192.168.4.127.1026.0.0.0.0.0 (integer) listen(2)
 257: tcpConnState.192.168.27.139.9.0.0.0.0.0 (integer) listen(2)
 258: tcpConnState.192.168.4.127.9.0.0.0.0.0 (integer) listen(2)
 259: tcpConnState.192.168.27.139.111.0.0.0.0.0 (integer) listen(2)
 260: tcpConnState.192.168.4.127.111.0.0.0.0.0 (integer) listen(2)
 261: tcpConnState.192.168.27.139.80.0.0.0.0.0 (integer) listen(2)
 262: tcpConnState.192.168.4.127.80.0.0.0.0.0 (integer) listen(2)
 263: tcpConnState.192.168.27.139.21.0.0.0.0.0 (integer) listen(2)
 264: tcpConnState.192.168.4.127.21.0.0.0.0.0 (integer) listen(2)
 265: tcpConnState.192.168.27.139.22.0.0.0.0.0 (integer) listen(2)
 266: tcpConnState.192.168.4.127.22.0.0.0.0.0 (integer) listen(2)
 267: tcpConnState.192.168.27.139.23.0.0.0.0.0 (integer) listen(2)
 268: tcpConnState.192.168.4.127.23.0.0.0.0.0 (integer) listen(2)
 269: tcpConnLocalAddress.192.168.27.139.1024.0.0.0.0 (ipaddress) 192.168.27.139
 270: tcpConnLocalAddress.192.168.4.127.1024.0.0.0.0 (ipaddress) 192.168.4.127

271: tcpConnLocalAddress.192.168.27.139.1025.0.0.0.0.0 (ipaddress) 192.168.27.139
272: tcpConnLocalAddress.192.168.4.127.1025.0.0.0.0.0 (ipaddress) 192.168.4.127
273: tcpConnLocalAddress.192.168.27.139.2049.0.0.0.0.0 (ipaddress) 192.168.27.139
274: tcpConnLocalAddress.192.168.4.127.2049.0.0.0.0.0 (ipaddress) 192.168.4.127
275: tcpConnLocalAddress.192.168.27.139.1026.0.0.0.0.0 (ipaddress) 192.168.27.139
276: tcpConnLocalAddress.192.168.4.127.1026.0.0.0.0.0 (ipaddress) 192.168.4.127
277: tcpConnLocalAddress.192.168.27.139.9.0.0.0.0.0 (ipaddress) 192.168.27.139
278: tcpConnLocalAddress.192.168.4.127.9.0.0.0.0.0 (ipaddress) 192.168.4.127
279: tcpConnLocalAddress.192.168.27.139.111.0.0.0.0.0 (ipaddress) 192.168.27.139
280: tcpConnLocalAddress.192.168.4.127.111.0.0.0.0.0 (ipaddress) 192.168.4.127
281: tcpConnLocalAddress.192.168.27.139.80.0.0.0.0.0 (ipaddress) 192.168.27.139
282: tcpConnLocalAddress.192.168.4.127.80.0.0.0.0.0 (ipaddress) 192.168.4.127
283: tcpConnLocalAddress.192.168.27.139.21.0.0.0.0.0 (ipaddress) 192.168.27.139
284: tcpConnLocalAddress.192.168.4.127.21.0.0.0.0.0 (ipaddress) 192.168.4.127
285: tcpConnLocalAddress.192.168.27.139.22.0.0.0.0.0 (ipaddress) 192.168.27.139
286: tcpConnLocalAddress.192.168.4.127.22.0.0.0.0.0 (ipaddress) 192.168.4.127
287: tcpConnLocalAddress.192.168.27.139.23.0.0.0.0.0 (ipaddress) 192.168.27.139
288: tcpConnLocalAddress.192.168.4.127.23.0.0.0.0.0 (ipaddress) 192.168.4.127
289: tcpConnLocalPort.192.168.27.139.1024.0.0.0.0.0 (integer) 1024
290: tcpConnLocalPort.192.168.4.127.1024.0.0.0.0.0 (integer) 1024
291: tcpConnLocalPort.192.168.27.139.1025.0.0.0.0.0 (integer) 1025
292: tcpConnLocalPort.192.168.4.127.1025.0.0.0.0.0 (integer) 1025
293: tcpConnLocalPort.192.168.27.139.2049.0.0.0.0.0 (integer) 2049
294: tcpConnLocalPort.192.168.4.127.2049.0.0.0.0.0 (integer) 2049
295: tcpConnLocalPort.192.168.27.139.1026.0.0.0.0.0 (integer) 1026
296: tcpConnLocalPort.192.168.4.127.1026.0.0.0.0.0 (integer) 1026
297: tcpConnLocalPort.192.168.27.139.9.0.0.0.0.0 (integer) 9
298: tcpConnLocalPort.192.168.4.127.9.0.0.0.0.0 (integer) 9
299: tcpConnLocalPort.192.168.27.139.111.0.0.0.0.0 (integer) 111
300: tcpConnLocalPort.192.168.4.127.111.0.0.0.0.0 (integer) 111
301: tcpConnLocalPort.192.168.27.139.80.0.0.0.0.0 (integer) 80
302: tcpConnLocalPort.192.168.4.127.80.0.0.0.0.0 (integer) 80
303: tcpConnLocalPort.192.168.27.139.21.0.0.0.0.0 (integer) 21
304: tcpConnLocalPort.192.168.4.127.21.0.0.0.0.0 (integer) 21
305: tcpConnLocalPort.192.168.27.139.22.0.0.0.0.0 (integer) 22
306: tcpConnLocalPort.192.168.4.127.22.0.0.0.0.0 (integer) 22
307: tcpConnLocalPort.192.168.27.139.23.0.0.0.0.0 (integer) 23
308: tcpConnLocalPort.192.168.4.127.23.0.0.0.0.0 (integer) 23
309: tcpConnRemAddress.192.168.27.139.1024.0.0.0.0.0 (ipaddress) 0.0.0.0
310: tcpConnRemAddress.192.168.4.127.1024.0.0.0.0.0 (ipaddress) 0.0.0.0
311: tcpConnRemAddress.192.168.27.139.1025.0.0.0.0.0 (ipaddress) 0.0.0.0
312: tcpConnRemAddress.192.168.4.127.1025.0.0.0.0.0 (ipaddress) 0.0.0.0
313: tcpConnRemAddress.192.168.27.139.2049.0.0.0.0.0 (ipaddress) 0.0.0.0
314: tcpConnRemAddress.192.168.4.127.2049.0.0.0.0.0 (ipaddress) 0.0.0.0
315: tcpConnRemAddress.192.168.27.139.1026.0.0.0.0.0 (ipaddress) 0.0.0.0
316: tcpConnRemAddress.192.168.4.127.1026.0.0.0.0.0 (ipaddress) 0.0.0.0
317: tcpConnRemAddress.192.168.27.139.9.0.0.0.0.0 (ipaddress) 0.0.0.0
318: tcpConnRemAddress.192.168.4.127.9.0.0.0.0.0 (ipaddress) 0.0.0.0
319: tcpConnRemAddress.192.168.27.139.111.0.0.0.0.0 (ipaddress) 0.0.0.0
320: tcpConnRemAddress.192.168.4.127.111.0.0.0.0.0 (ipaddress) 0.0.0.0
321: tcpConnRemAddress.192.168.27.139.80.0.0.0.0.0 (ipaddress) 0.0.0.0
322: tcpConnRemAddress.192.168.4.127.80.0.0.0.0.0 (ipaddress) 0.0.0.0
323: tcpConnRemAddress.192.168.27.139.21.0.0.0.0.0 (ipaddress) 0.0.0.0
324: tcpConnRemAddress.192.168.4.127.21.0.0.0.0.0 (ipaddress) 0.0.0.0
325: tcpConnRemAddress.192.168.27.139.22.0.0.0.0.0 (ipaddress) 0.0.0.0
326: tcpConnRemAddress.192.168.4.127.22.0.0.0.0.0 (ipaddress) 0.0.0.0
327: tcpConnRemAddress.192.168.27.139.23.0.0.0.0.0 (ipaddress) 0.0.0.0
328: tcpConnRemAddress.192.168.4.127.23.0.0.0.0.0 (ipaddress) 0.0.0.0
329: tcpConnRemPort.192.168.27.139.1024.0.0.0.0.0 (integer) 0
330: tcpConnRemPort.192.168.4.127.1024.0.0.0.0.0 (integer) 0
331: tcpConnRemPort.192.168.27.139.1025.0.0.0.0.0 (integer) 0
332: tcpConnRemPort.192.168.4.127.1025.0.0.0.0.0 (integer) 0
333: tcpConnRemPort.192.168.27.139.2049.0.0.0.0.0 (integer) 0
334: tcpConnRemPort.192.168.4.127.2049.0.0.0.0.0 (integer) 0
335: tcpConnRemPort.192.168.27.139.1026.0.0.0.0.0 (integer) 0
336: tcpConnRemPort.192.168.4.127.1026.0.0.0.0.0 (integer) 0
337: tcpConnRemPort.192.168.27.139.9.0.0.0.0.0 (integer) 0

338: tcpConnRemPort.192.168.4.127.9.0.0.0.0.0 (integer) 0
339: tcpConnRemPort.192.168.27.139.111.0.0.0.0.0 (integer) 0
340: tcpConnRemPort.192.168.4.127.111.0.0.0.0.0 (integer) 0
341: tcpConnRemPort.192.168.27.139.80.0.0.0.0.0 (integer) 0
342: tcpConnRemPort.192.168.4.127.80.0.0.0.0.0 (integer) 0
343: tcpConnRemPort.192.168.27.139.21.0.0.0.0.0 (integer) 0
344: tcpConnRemPort.192.168.4.127.21.0.0.0.0.0 (integer) 0
345: tcpConnRemPort.192.168.27.139.22.0.0.0.0.0 (integer) 0
346: tcpConnRemPort.192.168.4.127.22.0.0.0.0.0 (integer) 0
347: tcpConnRemPort.192.168.27.139.23.0.0.0.0.0 (integer) 0
348: tcpConnRemPort.192.168.4.127.23.0.0.0.0.0 (integer) 0
349: tcpInErrs.0 (counter) 6
350: tcpOutRsts.0 (counter) 37224
351: udpInDatagrams.0 (counter) 434
352: udpNoPorts.0 (counter) 8
353: udpInErrors.0 (counter) 0
354: udpOutDatagrams.0 (counter) 903
355: udpLocalAddress.192.168.27.139.1024 (ipaddress) 192.168.27.139
356: udpLocalAddress.192.168.4.127.1024 (ipaddress) 192.168.4.127
357: udpLocalAddress.192.168.27.139.2049 (ipaddress) 192.168.27.139
358: udpLocalAddress.192.168.4.127.2049 (ipaddress) 192.168.4.127
359: udpLocalAddress.192.168.27.139.1026 (ipaddress) 192.168.27.139
360: udpLocalAddress.192.168.4.127.1026 (ipaddress) 192.168.4.127
361: udpLocalAddress.192.168.27.139.1027 (ipaddress) 192.168.27.139
362: udpLocalAddress.192.168.4.127.1027 (ipaddress) 192.168.4.127
363: udpLocalAddress.192.168.27.139.9 (ipaddress) 192.168.27.139
364: udpLocalAddress.192.168.4.127.9 (ipaddress) 192.168.4.127
365: udpLocalAddress.192.168.27.139.161 (ipaddress) 192.168.27.139
366: udpLocalAddress.192.168.4.127.161 (ipaddress) 192.168.4.127
367: udpLocalAddress.192.168.27.139.4800 (ipaddress) 192.168.27.139
368: udpLocalAddress.192.168.4.127.4800 (ipaddress) 192.168.4.127
369: udpLocalAddress.192.168.27.139.854 (ipaddress) 192.168.27.139
370: udpLocalAddress.192.168.4.127.854 (ipaddress) 192.168.4.127
371: udpLocalAddress.192.168.27.139.111 (ipaddress) 192.168.27.139
372: udpLocalAddress.192.168.4.127.111 (ipaddress) 192.168.4.127
373: udpLocalPort.192.168.27.139.1024 (integer) 1024
374: udpLocalPort.192.168.4.127.1024 (integer) 1024
375: udpLocalPort.192.168.27.139.2049 (integer) 2049
376: udpLocalPort.192.168.4.127.2049 (integer) 2049
377: udpLocalPort.192.168.27.139.1026 (integer) 1026
378: udpLocalPort.192.168.4.127.1026 (integer) 1026
379: udpLocalPort.192.168.27.139.1027 (integer) 1027
380: udpLocalPort.192.168.4.127.1027 (integer) 1027
381: udpLocalPort.192.168.27.139.9 (integer) 9
382: udpLocalPort.192.168.4.127.9 (integer) 9
383: udpLocalPort.192.168.27.139.161 (integer) 161
384: udpLocalPort.192.168.4.127.161 (integer) 161
385: udpLocalPort.192.168.27.139.4800 (integer) 4800
386: udpLocalPort.192.168.4.127.4800 (integer) 4800
387: udpLocalPort.192.168.27.139.854 (integer) 854
388: udpLocalPort.192.168.4.127.854 (integer) 854
389: udpLocalPort.192.168.27.139.111 (integer) 111
390: udpLocalPort.192.168.4.127.111 (integer) 111
391: rs232Number.0 (integer) 4
392: rs232PortIndex.1 (integer) 1 [1]
393: rs232PortIndex.2 (integer) 2 [2]
394: rs232PortIndex.3 (integer) 3 [3]
395: rs232PortIndex.4 (integer) 4 [4]
396: rs232PortType.1 (integer) rs232(2)
397: rs232PortType.2 (integer) rs232(2)
398: rs232PortType.3 (integer) rs232(2)
399: rs232PortType.4 (integer) rs232(2)
400: rs232PortInSigNumber.1 (integer) 3
401: rs232PortInSigNumber.2 (integer) 3
402: rs232PortInSigNumber.3 (integer) 3
403: rs232PortInSigNumber.4 (integer) 3
404: rs232PortOutSigNumber.1 (integer) 2

405: rs232PortOutSigNumber.2 (integer) 2
406: rs232PortOutSigNumber.3 (integer) 2
407: rs232PortOutSigNumber.4 (integer) 2
408: rs232PortInSpeed.1 (integer) 38400
409: rs232PortInSpeed.2 (integer) 38400
410: rs232PortInSpeed.3 (integer) 38400
411: rs232PortInSpeed.4 (integer) 38400
412: rs232PortOutSpeed.1 (integer) 38400
413: rs232PortOutSpeed.2 (integer) 38400
414: rs232PortOutSpeed.3 (integer) 38400
415: rs232PortOutSpeed.4 (integer) 38400
416: rs232AsyncPortIndex.1 (integer) 1 [1]
417: rs232AsyncPortIndex.2 (integer) 2 [2]
418: rs232AsyncPortIndex.3 (integer) 3 [3]
419: rs232AsyncPortIndex.4 (integer) 4 [4]
420: rs232AsyncPortBits.1 (integer) 8
421: rs232AsyncPortBits.2 (integer) 8
422: rs232AsyncPortBits.3 (integer) 8
423: rs232AsyncPortBits.4 (integer) 8
424: rs232AsyncPortStopBits.1 (integer) one(1)
425: rs232AsyncPortStopBits.2 (integer) one(1)
426: rs232AsyncPortStopBits.3 (integer) one(1)
427: rs232AsyncPortStopBits.4 (integer) one(1)
428: rs232AsyncPortParity.1 (integer) none(1)
429: rs232AsyncPortParity.2 (integer) none(1)
430: rs232AsyncPortParity.3 (integer) none(1)
431: rs232AsyncPortParity.4 (integer) none(1)
432: rs232InSigPortIndex.1.2 (integer) 1 [1]
433: rs232InSigPortIndex.2.2 (integer) 2 [2]
434: rs232InSigPortIndex.3.2 (integer) 3 [3]
435: rs232InSigPortIndex.4.2 (integer) 4 [4]
436: rs232InSigPortIndex.1.3 (integer) 1 [1]
437: rs232InSigPortIndex.2.3 (integer) 2 [2]
438: rs232InSigPortIndex.3.3 (integer) 3 [3]
439: rs232InSigPortIndex.4.3 (integer) 4 [4]
440: rs232InSigPortIndex.1.6 (integer) 1 [1]
441: rs232InSigPortIndex.2.6 (integer) 2 [2]
442: rs232InSigPortIndex.3.6 (integer) 3 [3]
443: rs232InSigPortIndex.4.6 (integer) 4 [4]
444: rs232InSigName.1.2 (integer) cts(2)
445: rs232InSigName.2.2 (integer) cts(2)
446: rs232InSigName.3.2 (integer) cts(2)
447: rs232InSigName.4.2 (integer) cts(2)
448: rs232InSigName.1.3 (integer) dsr(3)
449: rs232InSigName.2.3 (integer) dsr(3)
450: rs232InSigName.3.3 (integer) dsr(3)
451: rs232InSigName.4.3 (integer) dsr(3)
452: rs232InSigName.1.6 (integer) dcd(6)
453: rs232InSigName.2.6 (integer) dcd(6)
454: rs232InSigName.3.6 (integer) dcd(6)
455: rs232InSigName.4.6 (integer) dcd(6)
456: rs232InSigState.1.2 (integer) off(3)
457: rs232InSigState.2.2 (integer) off(3)
458: rs232InSigState.3.2 (integer) off(3)
459: rs232InSigState.4.2 (integer) off(3)
460: rs232InSigState.1.3 (integer) off(3)
461: rs232InSigState.2.3 (integer) off(3)
462: rs232InSigState.3.3 (integer) off(3)
463: rs232InSigState.4.3 (integer) off(3)
464: rs232InSigState.1.6 (integer) off(3)
465: rs232InSigState.2.6 (integer) off(3)
466: rs232InSigState.3.6 (integer) off(3)
467: rs232InSigState.4.6 (integer) off(3)
468: rs232OutSigPortIndex.1.1 (integer) 1 [1]
469: rs232OutSigPortIndex.2.1 (integer) 2 [2]
470: rs232OutSigPortIndex.3.1 (integer) 3 [3]
471: rs232OutSigPortIndex.4.1 (integer) 4 [4]

```
472: rs232OutSigPortIndex.1.4 (integer) 1 [1]
473: rs232OutSigPortIndex.2.4 (integer) 2 [2]
474: rs232OutSigPortIndex.3.4 (integer) 3 [3]
475: rs232OutSigPortIndex.4.4 (integer) 4 [4]
476: rs232OutSigName.1.1 (integer) rts(1)
477: rs232OutSigName.2.1 (integer) rts(1)
478: rs232OutSigName.3.1 (integer) rts(1)
479: rs232OutSigName.4.1 (integer) rts(1)
480: rs232OutSigName.1.4 (integer) dtr(4)
481: rs232OutSigName.2.4 (integer) dtr(4)
482: rs232OutSigName.3.4 (integer) dtr(4)
483: rs232OutSigName.4.4 (integer) dtr(4)
484: rs232OutSigState.1.1 (integer) off(3)
485: rs232OutSigState.2.1 (integer) off(3)
486: rs232OutSigState.3.1 (integer) off(3)
487: rs232OutSigState.4.1 (integer) off(3)
488: rs232OutSigState.1.4 (integer) off(3)
489: rs232OutSigState.2.4 (integer) off(3)
490: rs232OutSigState.3.4 (integer) off(3)
491: rs232OutSigState.4.4 (integer) off(3)
492: snmpInPkts.0 (counter) 493
493: snmpOutPkts.0 (counter) 493
494: snmpInBadVersions.0 (counter) 0
495: snmpInBadCommunityNames.0 (counter) 0
496: snmpInBadCommunityUses.0 (counter) 0
497: snmpInASNParseErrs.0 (counter) 0
498: snmpInTooBigs.0 (counter) 0
499: snmpInNoSuchNames.0 (counter) 0
500: snmpInBadValues.0 (counter) 0
501: snmpInReadOnly.0 (counter) 0
502: snmpInGenErrs.0 (counter) 0
503: snmpInTotalReqVars.0 (counter) 503
504: snmpInTotalSetVars.0 (counter) 0
505: snmpInGetRequests.0 (counter) 0
506: snmpInGetNexts.0 (counter) 506
507: snmpInSetRequests.0 (counter) 0
508: snmpInGetResponses.0 (counter) 0
509: snmpInTraps.0 (counter) 0
510: snmpOutTooBigs.0 (counter) 0
511: snmpOutNoSuchNames.0 (counter) 0
512: snmpOutBadValues.0 (counter) 0
513: snmpOutGenErrs.0 (counter) 0
514: snmpOutGetRequests.0 (counter) 0
515: snmpOutGetNexts.0 (counter) 0
516: snmpOutSetRequests.0 (counter) 0
517: snmpOutGetResponses.0 (counter) 517
518: snmpOutTraps.0 (counter) 0
519: snmpEnableAuthenTraps.0 (integer) disabled(2)
**** SNMP QUERY FINISHED ****
```

NOTE Click on the following links for more information about MIB II and RS-232 like groups:

<http://www.faqs.org/rfcs/rfc1213.html>

<http://www.faqs.org/rfcs/rfc1317.html>

→ W311/321/341 do NOT support SNMP trap.

OpenVPN

OpenVPN provides two types of tunnels for users to implement VPNS: **Routed IP Tunnels** and **Bridged Ethernet Tunnels**. To begin with, check to make sure that the system has a virtual device `/dev/net/tun`. If not, issue the following command:

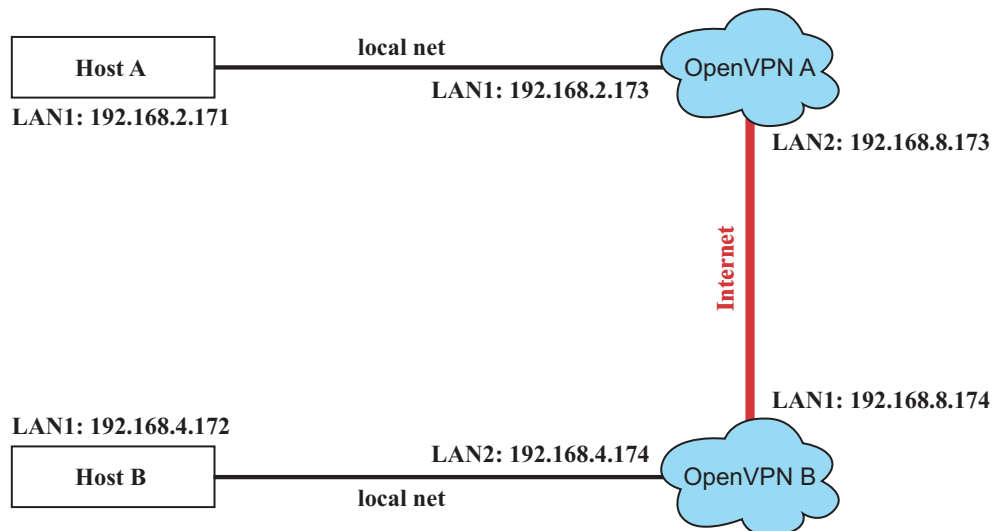
```
# mknod /dev/net/tun c 10 200
```

An Ethernet bridge is used to connect different Ethernet networks together. The Ethernets are bundled into one bigger, “logical” Ethernet. Each Ethernet corresponds to one physical interface (or port) that is connected to the bridge.

On each OpenVPN machine, you should generate a working directory, such as `/etc/openvpn`, where script files and key files reside. Once established, all operations will be performed in that directory.

Setup 1: Ethernet Bridging for Private Networks on Different Subnets

1. Set up four machines, as shown in the following diagram.



Host A (B) represents one of the machines that belongs to OpenVPN A (B). The two remote subnets are configured for a different range of IP addresses. When this setup is moved to a public network, the external interfaces of the OpenVPN machines should be configured for static IPs, or connect to another device (such as a firewall or DSL box) first.

```
# openvpn --genkey --secret secrouter.key
```

Copy the file that is generated to the OpenVPN machine.

2. Generate a script file named `openvpn-bridge` on each OpenVPN machine. This script reconfigures interface “eth1” as IP-less, creates logical bridge(s) and TAP interfaces, loads modules, enables IP forwarding, etc.

```
#-----start-----
#!/bin/sh

iface=eth1 # defines the internal interface
maxtap=`expr 1` # defines the number of tap devices. I.e., # of tunnels

IPADDR=
```

```

NETMASK=
BROADCAST=

# it is not a great idea but this system doesn't support
# /etc/sysconfig/network-scripts/ifcfg-eth1
ifcfg_vpn()
{
while read f1 f2 f3 f4 r3
do
if [ "$f1" = "iface" -a "$f2" = "$iface" -a "$f3" = "inet" -a "$f4" = "static" ];then
i=`expr 0`
while :
do
if [ $i -gt 5 ]; then
break
fi
i=`expr $i + 1`
read f1 f2
case "$f1" in
address ) IPADDR=$f2
;;
netmask ) NETMASK=$f2
;;
broadcast ) BROADCAST=$f2
;;
esac
done
break
fi
done < /etc/network/interfaces
}

# get the ip address of the specified interface
mname=
module_up()
{
oIFS=$IFS
IFS=`
`
FOUND="no"
for LINE in `lsmod`
do
TOK=`echo $LINE | cut -d' ' -f1`
if [ "$TOK" = "$mname" ]; then
FOUND="yes";
break;
fi
done
IFS=$oIFS

if [ "$FOUND" = "no" ]; then
modprobe $mname
fi
}

start()
{
ifcfg_vpn
if [ ! \( -d "/dev/net" \) ]; then
mkdir /dev/net
fi

if [ ! \( -r "/dev/net/tun" \) ]; then
# create a device file if there is none
mknod /dev/net/tun c 10 200
fi

# load modules "tun" and "bridge"

```

```
mname=tun
module_up
mname=bridge
module_up
# create an ethernet bridge to connect tap devices, internal interface
brctl addbr br0
brctl addif br0 $iface
# the bridge receives data from any port and forwards it to other ports.

i=`expr 0`
while :
do
# generate a tap0 interface on tun
openvpn --mktun --dev tap${i}

# connect tap device to the bridge
brctl addif br0 tap${i}

# null ip address of tap device
ifconfig tap${i} 0.0.0.0 promisc up

i=`expr $i + 1`
if [ $i -ge $maxtap ]; then
break
fi
done

# null ip address of internal interface
ifconfig $iface 0.0.0.0 promisc up

# enable bridge ip
ifconfig br0 $IPADDR netmask $NETMASK broadcast $BROADCAST

ipf=/proc/sys/net/ipv4/ip_forward
# enable IP forwarding
echo 1 > $ipf
echo "ip forwarding enabled to"
cat $ipf
}

stop() {
echo "shutdown openvpn bridge."
ifcfg_vpn
i=`expr 0`
while :
do
# disconnect tap device from the bridge
brctl delif br0 tap${i}
openvpn --rmtun --dev tap${i}

i=`expr $i + 1`
if [ $i -ge $maxtap ]; then
break
fi
done
brctl delif br0 $iface
brctl delbr br0
ifconfig br0 down
ifconfig $iface $IPADDR netmask $NETMASK broadcast $BROADCAST
killall -TERM openvpn
}

case "$1" in
start)
start
;;
stop)
stop
;
```

```

;;
restart)
stop
start
;;
*)
echo "Usage: $0 [start|stop|restart]"
exit 1
esac
exit 0
#----- end -----

```

Create link symbols to enable this script at boot time:

```

# ln -s /etc/openvpn/openvpn-bridge /etc/rc.d/rc3.d/S32vpn-br # for example
# ln -s /etc/openvpn/openvpn-bridge /etc/rc.d/rc6.d/K32vpn-br # for example

```

3. Create a configuration file named **A-tap0-br.conf** and an executable script file named **A-tap0-br.sh** on OpenVPN A.

```

# point to the peer
remote 192.168.8.174
dev tap0
secret /etc/openvpn/secrouter.key
cipher DES-EDE3-CBC
auth MD5
tun-mtu 1500
tun-mtu-extra 64
ping 40
up /etc/openvpn/A-tap0-br.sh

#-----Start-----
#!/bin/sh
# value after "-net" is the subnet behind the remote peer
route add -net 192.168.4.0 netmask 255.255.255.0 dev br0
#----- end -----

```

Create a configuration file named **B-tap0-br.conf** and an executable script file named **B-tap0-br.sh** on OpenVPN B.

```

# point to the peer
remote 192.168.8.173
dev tap0
secret /etc/openvpn/secrouter.key
cipher DES-EDE3-CBC
auth MD5
tun-mtu 1500
tun-mtu-extra 64
ping 40
up /etc/openvpn/B-tap0-br.sh

#----- Start-----
#!/bin/sh
# value after "-net" is the subnet behind the remote peer
route add -net 192.168.2.0 netmask 255.255.255.0 dev br0
#----- end -----

```

Note: Select cipher and authentication algorithms by specifying “cipher” and “auth”. To see with algorithms are available, type:

```

# openvpn --show-ciphers
# openvpn --show-auths

```

4. Start both of OpenVPN peers,

```

# openvpn --config A-tap0-br.conf&
# openvpn --config B-tap0-br.conf&

```

If you see the line “Peer Connection Initiated with 192.168.8.173:5000” on each machine, the connection between OpenVPN machines has been established successfully on UDP port 5000.

5. On each OpenVPN machine, check the routing table by typing the command:

```
# route
```

| Destination | Gateway | Genmsk | Flags | Metric | Ref | Use | Iface |
|-------------|---------|---------------|-------|--------|-----|-----|-------|
| 192.168.4.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | br0 |
| 192.168.2.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | br0 |
| 192.168.8.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |

Interface **eth1** is connected to the bridging interface **br0**, to which device **tap0** also connects, whereas the virtual device **tun** sits on top of **tap0**. This ensures that all traffic from internal networks connected to interface **eth1** that come to this bridge write to the TAP/TUN device that the OpenVPN program monitors. Once the OpenVPN program detects traffic on the virtual device, it sends the traffic to its peer.

6. To create an indirect connection to Host B from Host A, you need to add the following routing item:

```
route add -net 192.168.4.0 netmask 255.255.255.0 dev eth0
```

To create an indirect connection to Host A from Host B, you need to add the following routing item:

```
route add -net 192.168.2.0 netmask 255.255.255.0 dev eth0
```

Now ping Host B from Host A by typing:

```
ping 192.168.4.174
```

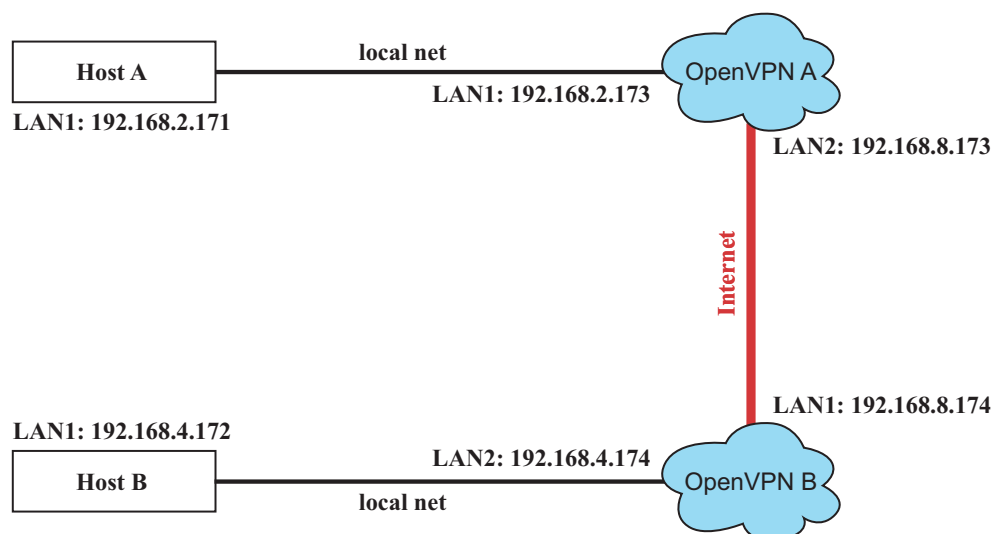
A successful ping indicates that you have created a VPN system that only allows authorized users from one internal network to access users at the remote site. For this system, all data is transmitted by UDP packets on port 5000 between OpenVPN peers.

7. To shut down OpenVPN programs, type the command:

```
# killall -TERM openvpn
```

Setup 2: Ethernet Bridging for Private Networks on the Same Subnet

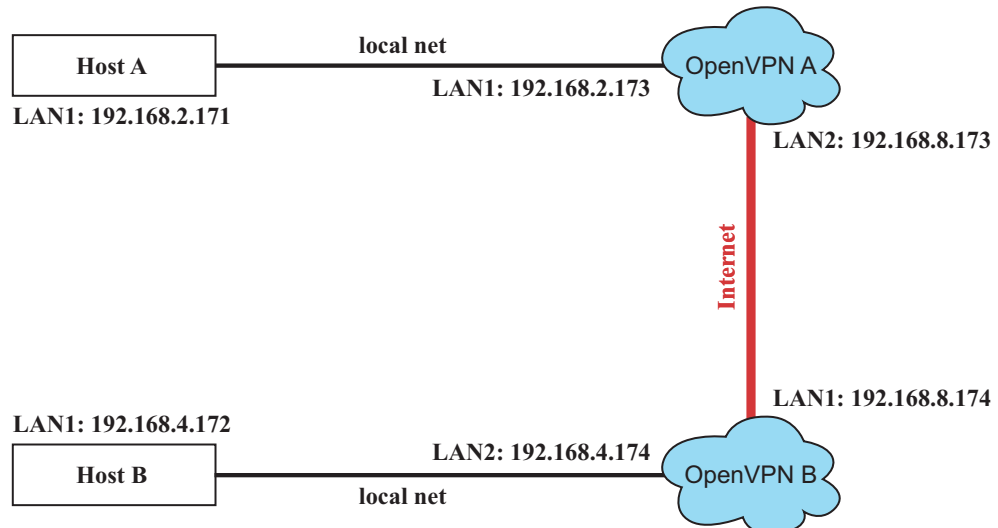
1. Set up four machines as shown in the following diagram:



- The configuration procedure is almost the same as for the previous example. The only difference is that you will need to comment out the parameter "up" in "/etc/openvpn/A-tap0-br.conf" and "/etc/openvpn/B-tap0-br.conf".

Setup 3: Routed IP

- Set up four machines as shown in the following diagram:



- Create a configuration file named "A-tun.conf" and an executable script file named "A-tun.sh".

```
# point to the peer
remote 192.168.8.174
dev tun
secret /etc/openvpn/secrouter.key
cipher DES-EDE3-CBC
auth MD5
tun-mtu 1500
tun-mtu-extra 64
ping 40
ifconfig 192.168.2.173 192.168.4.174
up /etc/openvpn/A-tun.sh
```

```
#----- Start-----
#!/bin/sh
# value after "-net" is the subnet behind the remote peer
route add -net 192.168.4.0 netmask 255.255.255.0 gw $5
#----- end -----
```

Create a configuration file named **B-tun.conf** and an executable script file named **B-tun.sh** on OpenVPN B:

```
remote 192.168.8.173
dev tun
secret /etc/openvpn/secrouter.key
cipher DES-EDE3-CBC
auth MD5
tun-mtu 1500
tun-mtu-extra 64
ping 40
ifconfig 192.168.4.174 192.168.2.173
up /etc/openvpn/B-tun.sh
```

```
#----- Start-----
#!/bin/sh
```



```
# value after "-net" is the subnet behind the remote peer
route add -net 192.168.2.0 netmask 255.255.255.0 gw $5
#----- end -----
```

Note that the parameter "ifconfig" defines the first argument as the local internal interface and the second argument as the internal interface at the remote peer.

Note that \$5 is the argument that the OpenVPN program passes to the script file. Its value is the second argument of **ifconfig** in the configuration file.

3. Check the routing table after you run the OpenVPN programs, by typing the command:

```
# route
```

| Destination | Gateway | Genmsk | Flags | Metric | Ref | Use | Iface |
|---------------|---------------|-----------------|-------|--------|-----|-----|-------|
| 192.168.4.174 | * | 255.255.255.255 | UH | 0 | 0 | 0 | tun0 |
| 192.168.4.0 | 192.168.4.174 | 255.255.255.0 | UG | 0 | 0 | 0 | tun0 |
| 192.168.2.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth1 |
| 192.168.8.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |

Tool Chains for Application Development

This chapter describes how to install a tool chain in the host computer that you use to develop your applications. In addition, the process of performing cross-platform development and debugging are also introduced. For clarity, the W311/321/341 embedded computer is called a target computer.

The following functions are covered in this chapter:

❑ **Linux Tool Chain**

- Steps for Installing the Linux Tool Chain
- Compilation for Applications
- On-Line Debugging with GDB

❑ **Windows Tool Chain**

- System Requirements for Windows Tool Chain
- Steps for Installing Windows Tool Chain
- Using the BASH Shell
- Compilation for Applications
- On-Line Debugging with Insight

Linux Tool Chain

The Linux tool chain contains a suite of cross compilers and other tools, as well as the libraries and header files that are necessary to compile your applications. These tool chain components must be installed in your host computer (PC) running Linux. We have confirmed that the following Linux distributions can be used to install the tool chain.

Fedora core 1 & 2.

Steps for Installing the Linux Tool Chain

The tool chain needs about 485 MB of hard disk space. To install it, follow the steps.

1. Insert the package CD into your PC and then issue the following commands:

```
#mount /dev/cdrom /mnt/cdrom
#sh /mnt/cdrom/tool-chain/linux/install.sh
```
2. Wait for the installation process to complete. This should take a few minutes.
3. Add the directory **/usr/local/arm-linux/bin** to your path. You can do this for the current login by issuing the following commands:

```
#export PATH="/usr/local/arm-linux/bin:$PATH"
```

Alternatively, you can add the same commands to **\$HOME/.bash_profile** to make it effective for all login sessions.

Compilation for Applications

To compile a simple C application, use the cross compiler instead of the regular compiler:

```
#arm-linux-gcc -o example -Wall -g -O2 example.c
#arm-linux-strip -s example
#arm-linux-gcc -ggdb -o example-debug example.c
```

Most of the cross compiler tools are the same as their native compiler counterparts, but with an additional prefix that specifies the target system. In the case of x86 environments, the prefix is **i386-linux-** and in the case of IA204/241 ARM boards, it is **arm-linux-**.

For example, the native C compiler is **gcc** and the cross C compiler for ARM in the W311/321/341 is **arm-linux-gcc**.

The following cross compiler tools are provided:

| | |
|----------|--|
| ar | Manages archives (static libraries) |
| as | Assembler |
| c++, g++ | C++ compiler |
| cpp | C preprocessor |
| gcc | C compiler |
| gdb | Debugger |
| ld | Linker |
| nm | Lists symbols from object files |
| objcopy | Copies and translates object files |
| objdump | Displays information about object files |
| ranlib | Generates indexes to archives (static libraries) |
| readelf | Displays information about ELF files |
| size | Lists object file section sizes |
| strings | Prints strings of printable characters from files (usually object files) |
| strip | Removes symbols and sections from object files (usually debugging information) |

On-Line Debugging with GDB

The tool chain also provides an on-line debugging mechanism to help you develop your program. Before performing a debugging session, add the option `-ggdb` to compile the program. A debugging session runs on a client-server architecture on which the server `gdbserver` is installed into the target computer and the client `ddd` is installed in the host computer. We'll assume that you have uploaded a program named `hello-debug` to the target computer and start to debug the program.

1. Log on to the target computer and run the debugging server program.

```
#gdbserver 192.168.4.142:2000 hello-debug
Process hello-debug created; pid=38
```

The debugging server listens for connections at network port 2000 from the network interface 192.168.4.142. The name of the program to be debugged follows these parameters. For a program requiring arguments, add the arguments behind the program name.

2. In the host computer, change the directory to where the program source resides.

```
cd /my_work_directory/myfilesystem/testprograms
```

3. Execute the client program.

```
#ddd --debugger arm-linux-gdb hello-debug &
```

4. Enter the following command at the GDB, DDD command prompt.

```
Target remote 192.168.4.99:2000
```

The command produces a line of output on the target console, similar to the following.

```
Remote debugging using 192.168.4.99:2000
```

192.168.4.99 is the machine's IP address, and 2000 is the port number. You can now begin debugging in the host environment using the interface provided by DDD.

5. Set a break point on main by double clicking, or by entering `b main` on the command line.
6. Click the **cont** button.

Windows Tool Chain

The Windows tool chain is a cross development environment that simulates the Linux root file system, allowing users to develop applications in a Windows PC environment. The following figure shows an example of what the tool chain looks like.

```
 /
Your group is currently "mkpasswd". This indicates that
The /etc/passwd (and possibly /etc/group) files should be rebuilt
See the man pages for mkpasswd and mkgroup then, for example, run
mkpasswd -l [-d] > /etc/passwd
mkpasswd -l [-d] > /etc/group
Note that the -d switch is necessary for domain users.

stephen_lin@abc-06d82fcbf1a /
$ ls -al
total 9
drwxr-xr-x  8 stephen_ mkpasswd    0 Jan 10 17:24 .
drwxr-xr-x  8 stephen_ mkpasswd    0 Jan 10 17:24 ..
drwxr-xr-x  2 stephen_ mkpasswd    0 Jan 10 19:48 bin
drwxr-xr-x  7 stephen_ mkpasswd    0 Jan 10 19:24 etc
-rw-r--r--  1 stephen_ mkpasswd  3262 Jan 10 22:03 insight.ico
drwxr-xr-x  5 stephen_ mkpasswd    0 Jan 10 19:48 lib
-rwxr-xr-x  1 stephen_ mkpasswd    53 Jan 10 22:03 moxa.bat
-rw-r--r--  1 stephen_ mkpasswd  3262 Jan 10 22:03 moxa.ico
drwxr-xr-x  2 stephen_ mkpasswd    0 Jan 10 19:48 tmp
drwxr-xr-x 14 stephen_ mkpasswd    0 Jan 10 19:48 usr
drwxr-xr-x  6 stephen_ mkpasswd    0 Jan 10 18:12 var

stephen_lin@abc-06d82fcbf1a /
$ _
```

System Requirements for Windows Tool Chain

Your Windows OS must satisfy the following requirements.

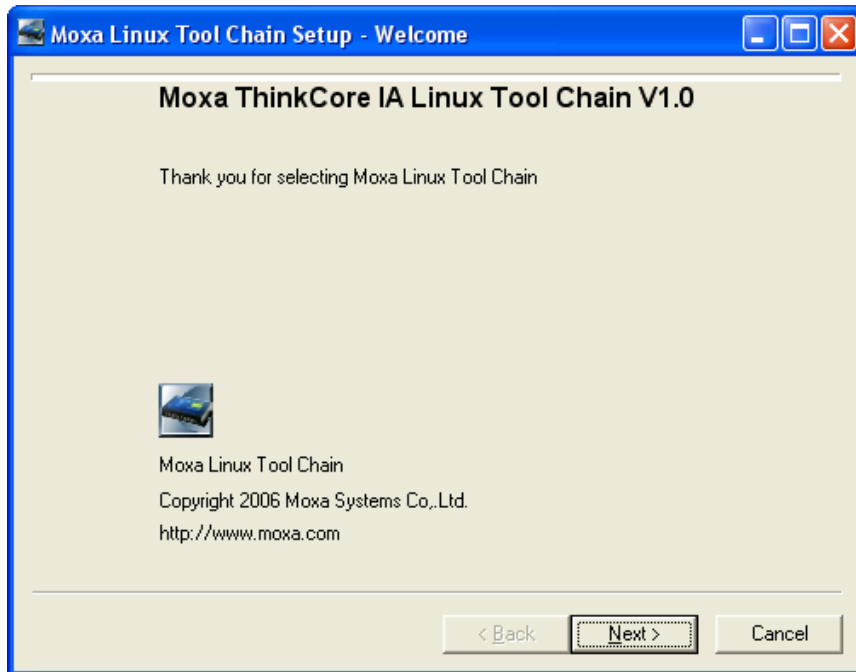
1. Windows 2000 workstation or Windows XP professional.
2. Minimum of 500 MB of free hard drive space on a single drive.
3. CD-ROM or equivalent.
4. Ethernet capability to upload application programs to the target computer.
5. Being able to log on as an administrator.
6. Windows username without spaces.

You will be using a BASH shell window to enter commands. In addition, for editing text files, such as configuration files, you should use vi editor. Do NOT use WordPad, which could cause problems when the files are transferred to a bona fide Linux environment.

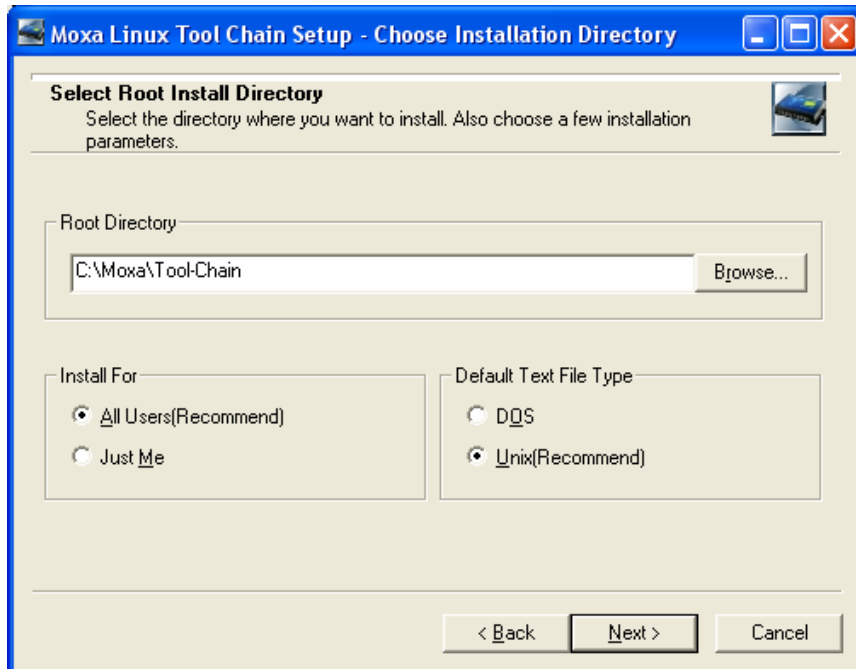
Steps for Installing Windows Tool Chain

If you have installed the old version of Windows Tool Chain or other Cygwin-related software, please remove these softwares and then follow the next procedure.

1. Double click on the tool chain file to start the installation process, and choose **Next**.

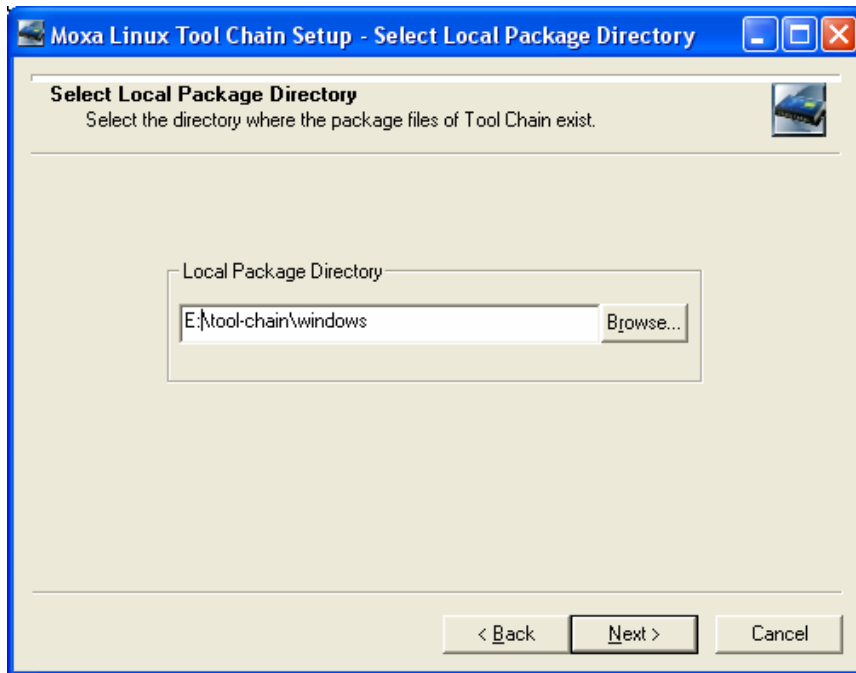


2. Browse to the directory where you prefer to set the root directory for the tool chain. Options of **All Users** and **Unix** are recommended. Then, choose **Next**.



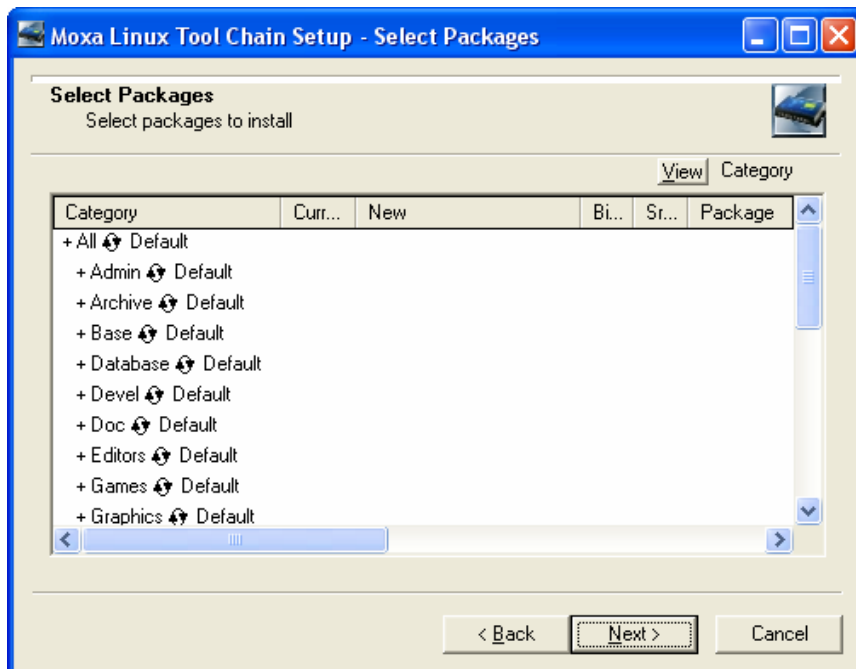
If you have installed a tool chain before, its root directory would show up in the **Root Directory** text field. If you continue the installation, the new tool chain in a previous root directory would override the old one. Choose a different directory to keep both tool chains.

3. Navigate to the directory where the packages of the tool chain reside. By default, it is on the CD-ROM: \\tool-chain\windows. Choose **Next** to proceed.



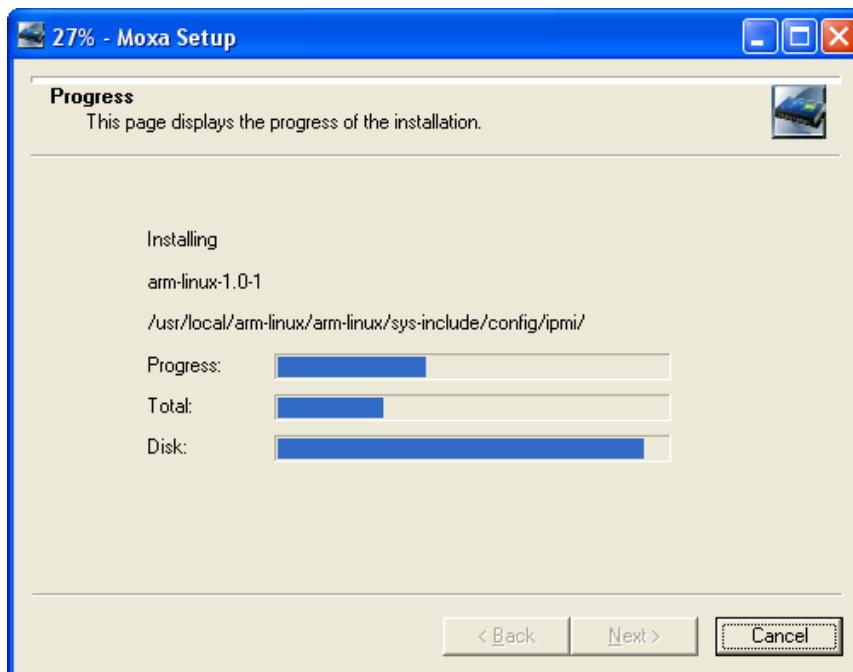
It may take anywhere from 5 to 20 minutes to check the packages in the CD-ROM.

4. All packages are selected by default. Choose **Next** to continue.

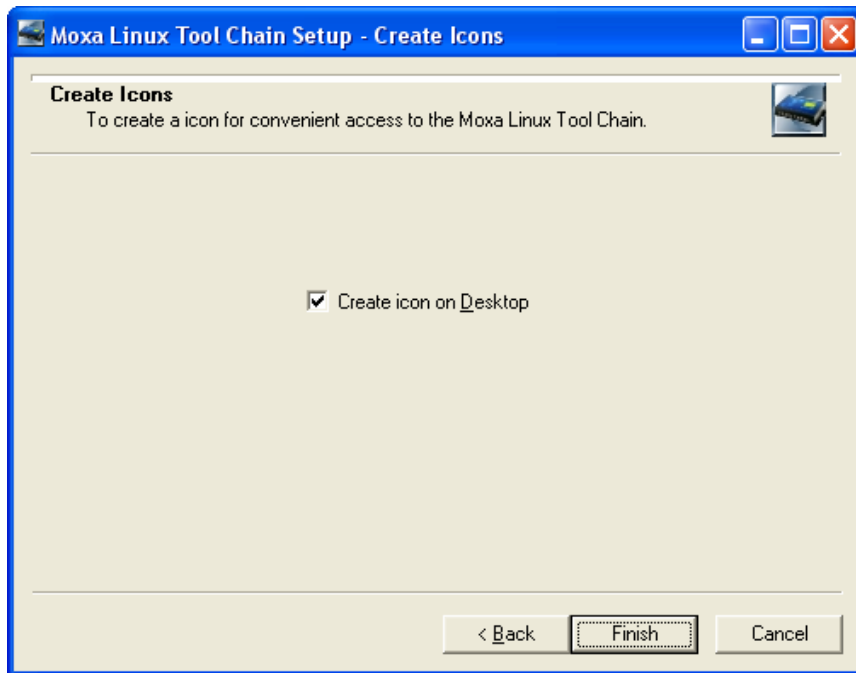


- **Category column:** Shows a hierarchical display of packages with category name highest and package name lowest. Click the plus sign (+) next to a category name to open the category and see the packages within that category.

- **Base Category:** List all packages that will be installed by default (along with any dependencies). If you view the Base column for the Base category, you should see every package selected for installation.
 - **Packages:** In the packages listing field, package names are arranged by Category/Full/Partial according to the **View by** button. When viewing by Category, click the plus sign (+) to open or close the packages under that category. This is the same list you see in flat form when viewing by Full/Partial. By default, named packages are installed.
 - **Install:** If the package was not previously installed, select this option to install the package now.
 - **Reinstall:** If the package was previously installed, select this option to install it again. This will overwrite the previous installation.
 - **Uninstall:** If the package was previously installed, select this option if you do NOT want to make any changes.
 - **Skip:** Ignores a package entirely, regardless of whether it was previously installed or uninstalled. Packages marked "Skip" are omitted from the Partial display.
5. The **Progress** window opens. The installer will install all packages that were selected. This process could take from 5 to 30 minutes, depending on the speed of your system. When the installation completes, the **Complete the Installation** window will appear.



6. Checkmark **Create icon on Desktop** to place a **Moxa BASH Shell** icon on your desktop, and then click on **Finish**.



7. Click on **OK** to complete the installation process.



Using the BASH Shell

A command-line interface is used to develop applications with the tool chain. To access the command line, you need to launch a BASH shell window.

To open a BASH shell window, choose **Start Menu → Programs → UC Tool Chain → Moxa Bash Shell**, or click on the desktop **Moxa Bash Shell** icon.

```
 /
Your group is currently "mkpasswd". This indicates that
The /etc/passwd (and possibly /etc/group) files should be rebuilt
See the man pages for mkpasswd and mkgroup then, for example, run
mkpasswd -l [-d] > /etc/passwd
mkpasswd -l [-d] > /etc/group
Note that the -d switch is necessary for domain users.

stephen_lin@abc-06d82fcbf1a /
$ ls -al
total 9
drwxr-xr-x  8 stephen_ mkpasswd    0 Jan 10 17:24 .
drwxr-xr-x  8 stephen_ mkpasswd    0 Jan 10 17:24 ..
drwxr-xr-x  2 stephen_ mkpasswd    0 Jan 10 19:48 bin
drwxr-xr-x  7 stephen_ mkpasswd    0 Jan 10 19:24 etc
-rw-r--r--  1 stephen_ mkpasswd  3262 Jan 10 22:03 insight.ico
drwxr-xr-x  5 stephen_ mkpasswd    0 Jan 10 19:48 lib
-rwxr-xr-x  1 stephen_ mkpasswd   53 Jan 10 22:03 moxa.bat
-rw-r--r--  1 stephen_ mkpasswd  3262 Jan 10 22:03 moxa.ico
drwxr-xr-x  2 stephen_ mkpasswd    0 Jan 10 19:48 tmp
drwxr-xr-x 14 stephen_ mkpasswd    0 Jan 10 19:48 usr
drwxr-xr-x  6 stephen_ mkpasswd    0 Jan 10 18:12 var

stephen_lin@abc-06d82fcbf1a /
$ _
```

Compilation for Applications

Windows tool chain is a cross compiler that can be used to compile Linux source code on a Windows operating system, allowing programmers to develop projects on a Windows-based PC. In this section, we describe the procedures you should follow to compile a project with the Windows tool chain.

First, copy the source code of your project in the Windows tool chain's installation directory. In the example shown here, we want to compile the hello example provided in our CD-ROM. We will copy the source code to /UC which is the root directory of the Windows tool chain. Check the root directory, where you can find the hello directory.

```
 /
Mkpasswd -l [-d] > /etc/passwd
Mkgroup -l [-d] > /etc/group
Note that the -d switch is necessary for domain users.

Jared_Wu@Jared_Wu ~
$ cd /

Jared_Wu@Jared_Wu /
$ ls -al
total 9
drwxrwx--- 9 Jared_Wu 4294967295 0 Nov 4 18:11 .
drwxrwx--- 9 Jared_Wu 4294967295 0 Nov 4 18:11 ..
drwxrwx--- 2 Jared_Wu 4294967295 0 Nov 4 11:10 bin
drwxrwx--- 7 Jared_Wu 4294967295 0 Nov 4 11:10 etc
drwx----- 2 Jared_Wu mkpasswd 0 Nov 4 18:07 hello
-rwxr-x--- 1 Jared_Wu 4294967295 3262 Nov 4 11:12 insight.ico
drwxrwx--- 5 Jared_Wu 4294967295 0 Nov 4 11:10 lib
-rwxr-x--- 1 Jared_Wu 4294967295 53 Nov 4 10:12 moxa.bat
-rwxr-x--- 1 Jared_Wu 4294967295 3262 Nov 4 11:12 moxa.ico
drwxrwx--- 4 Jared_Wu 4294967295 0 Nov 4 18:11 tmp
drwxrwx--- 13 Jared_Wu 4294967295 0 Nov 4 11:06 usr
drwxrwx--- 6 Jared_Wu 4294967295 0 Nov 4 11:06 var

Jared_Wu@Jared_Wu /
$
```

Next, enter the hello directory and invoke the make program that will execute the compilation instructions written in the Makefile to compile the hello project.

```

/hello
drwxrwx--- 7 Jared_Wu 4294967295 0 Nov 4 11:10 etc
drwx----- 2 Jared_Wu mkpasswd 0 Nov 4 18:07 hello
-rwxr-x--- 1 Jared_Wu 4294967295 3262 Nov 4 11:12 insight.ico
drwxrwx--- 5 Jared_Wu 4294967295 0 Nov 4 11:10 lib
-rwxr-x--- 1 Jared_Wu 4294967295 53 Nov 4 10:12 moxa.bat
-rwxr-x--- 1 Jared_Wu 4294967295 3262 Nov 4 11:12 moxa.ico
drwxrwx--- 4 Jared_Wu 4294967295 0 Nov 4 18:11 tmp
drwxrwx--- 13 Jared_Wu 4294967295 0 Nov 4 11:06 usr
drwxrwx--- 6 Jared_Wu 4294967295 0 Nov 4 11:06 var

Jared_Wu@Jared_Wu /
$ cd hello/

Jared_Wu@Jared_Wu /hello
$ make
/usr/local/mxscaleb/bin/mxscaleb-gcc -o hello-release hello.c
/usr/local/mxscaleb/bin/mxscaleb-strip -s hello-release
/usr/local/mxscaleb/bin/mxscaleb-gcc -ggdb -o hello-debug hello.c

Jared_Wu@Jared_Wu /hello
$ ls
Makefile README hello-debug hello-release hello.c

Jared_Wu@Jared_Wu /hello
$
    
```

After that, use FTP to upload the executable file to the UC, and then run the executable.

```

/hello
ftp> bye

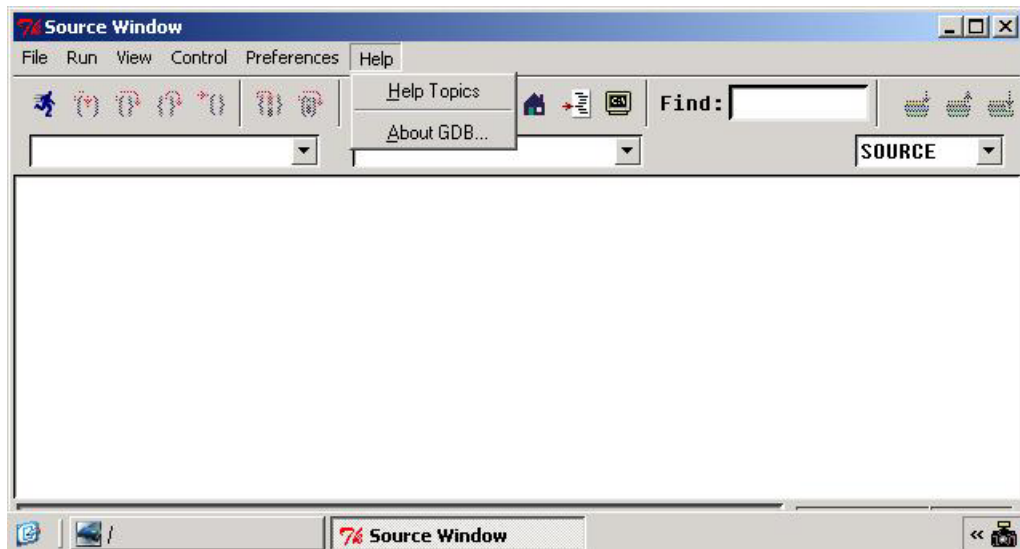
Jared_Wu@Jared_Wu /hello
$ ftp 192.168.14.9
Connected to 192.168.14.9.
220 Moxa FTP server <Version wu-2.6.1<2> Mon Nov 24 12:17:04 CST 2003> ready.
User <192.168.14.9:<none>>: root
331 Password required for root.
Password:
230 User root logged in.
ftp> bin
200 PORT command successful.
150 Opening BINARY mode data connection for hello-release.
226 Transfer complete.
ftp: 2744 bytes sent in 0.00Seconds 2744000.00Kbytes/sec.
ftp> bye
221-You have transferred 2744 bytes in 1 files.
221-Total traffic for this session was 3131 bytes in 1 transfers.
221-Thank you for using the FTP service on Moxa.
221 Goodbye.

Jared_Wu@Jared_Wu /hello
$
root@Moxa:~# chmod 777 hello-release
root@Moxa:~# ./hello-release
Hello
    
```

On-Line Debugging with Insight

Insight is a graphical user interface that accompanies **GDB**, the GNU Debugger was written in Tcl/Tk by people working at Red Hat, Inc., and Cygnus Solutions. Red Hat was generous enough to make Insight available for public use, and continues to maintain the program.

Click on <http://sources.redhat.com/insight/> for more information about using Insight, or click on **Help Topics** under the **Help** menu to read the user manual.



6

Programmer's Guide

This chapter includes important information for programmers.

The following functions are covered in this chapter:

- Flash Memory Map**
- Device API**
- RTC (Real Time Clock)**
- Buzzer**
- WDT (Watch Dog Timer)**
- UART**
- DO**

Flash Memory Map

Partition sizes are hard coded into the kernel binary. To change the partition sizes, you will need to rebuild the kernel. The flash memory map is shown in the following table.

| Address | Size | Contents |
|-------------------------|--------|-------------------------------------|
| 0x00000000 – 0x0003FFFF | 256 KB | Boot Loader—Read ONLY |
| 0x00040000 – 0x001FFFFF | 1.8 MB | Kernel object code—Read ONLY |
| 0x00200000 – 0x009FFFFF | 8 MB | Root file system (JFFS2) —Read ONLY |
| 0x00A00000 – 0x00FFFFFF | 6 MB | User directory (JFFS2) —Read/Write |

Mount the user file system to **/mnt/usrdisk** with the root file system. Check to see if the user file system was mounted correctly. If user file system is okay, the kernel will change the root file system to **/mnt/usrdisk**. If the user file system is not okay, the kernel will use the default Moxa file system. To finish boot process, run the init program.

- | | |
|------|---|
| NOTE | <ol style="list-style-type: none"> 1. The default Moxa file system only enables the network and CF. It lets users recover the user file system when it fails. 2. The user file system is a complete file system. Users can create and delete directories and files (including source code and executable files) as needed. 3. Users can create the user file system on the PC host or target platform, and then copy it to the W311/321/341. 4. To improve system performance, we strongly recommend that you install your application programs on the on-board flash. However, since the on-board flash has a fixed amount of free memory space, you must not over-write it, and instead use an external storage card, such as an SD or CF card, for the data log. |
|------|---|

Device API

The W311/321/341 support control devices with the **ioctl** system API. You will need to `include <moxadvice.h>`, and use the following **ioctl** function.

```
int ioctl(int d, int request,...);
Input: int d - open device node return file handle
      int request - argument in or out
```

Use the desktop Linux's man page for detailed documentation:

```
#man ioctl
```

RTC (Real Time Clock)

The device node is located at **/dev/rtc**. The W311/321/341 support Linux standard simple RTC control. You must `include <linux/rtc.h>`.

1. Function: **RTC_RD_TIME**

```
int ioctl(fd, RTC_RD_TIME, struct rtc_time *time);
```

 Description: read time information from RTC. It will return the value on argument 3.
2. Function: **RTC_SET_TIME**

```
int ioctl(fd, RTC_SET_TIME, struct rtc_time *time);
```

 Description: set RTC time. Argument 3 will be passed to RTC.

Buzzer

The device node is located at `/dev/console`. The W311/321/341 support Linux standard buzzer control, with the W311/321/341's buzzer running at a fixed frequency of 100 Hz. You must `include <sys/kd.h>`.

Function: KDMKTONE

```
ioctl(fd, KDMKTONE, unsigned int arg);
```

Description: The buzzer's behavior is determined by the argument `arg`. The "high word" part of `arg` gives the length of time the buzzer will sound, and the "low word" part gives the frequency.

The buzzer's on / off behavior is controlled by software. If you call the "ioctl" function, you MUST set the frequency at 100 Hz. If you use a different frequency, the system could crash.

WDT (Watch Dog Timer)

1. Introduction

The WDT works like a watch dog function. You can enable it or disable it. When the user enables WDT but the application does not acknowledge it, the system will reboot. You can set the ack time from a minimum of 50 msec to a maximum of 60 seconds.

2. How the WDT works

The sWatchDog is disabled when the system boots up. The user application can also enable ack. When the user does not ack, it will let the system reboot.

Kernel boot

.....
....

User application running and enable user ack

....
....

3. The user API

The user application must `include <moxadef.h>`, and `link moxalib.a`. A makefile example is shown below:

```
all:
    arm-linux-gcc -o xxxx xxxx.c -lmoxalib
```

```
int swtd_open(void)
```

Description

Open the file handle to control the sWatchDog. If you want to do something you must first to this. And keep the file handle to do other.

Input

None

Output

The return value is file handle. If has some error, it will return `< 0` value.

You can get error from `errno()`.


```
int swtd_enable(int fd, unsigned long time)
```

Description

Enable application sWatchDog. And you must do ack after this process.

Input

int fd - the file handle, from the swtd_open() return value.

unsigned long time - The time you wish to ack sWatchDog periodically. You must ack the sWatchDog before timeout. If you do not ack, the system will be reboot automatically. The minimal time is 50 msec, the maximum time is 60 seconds. The time unit is msec.

Output

OK will be zero. The other has some error, to get the error code from errno().

```
int swtd_disable(int fd)
```

Description

Disable the application to ack sWatchDog. And the kernel will be auto ack it. User does not to do it at periodic.

Input

int fd - the file handle from swtd_open() return value.

Output

OK will be zero. The other has some error, to get error code from errno.

```
int swtd_get(int fd, int *mode, unsigned long *time)
```

Description

Get current setting values.

mode -

1 for user application enable sWatchDog: need to do ack.

0 for user application disable sWatchdog: does not need to do ack.

time - The time period to ack sWatchDog.

Input :

int fd - the file handle from swtd_open() return value.

int *mode - the function will be return the status enable or disable user application need to do ack.

unsigned long *time - the function will return the current time period.

Output:

OK will be zero.

The other has some error, to get error code from errno().

```
int swtd_ack(int fd)
```

Description

Acknowledge sWatchDog. When the user application enable sWatchDog. It need to call this function periodically with user predefined time in the application program.

Input

int fd - the file handle from swtd_open() return value.

Output

OK will be zero.

The other has some error, to get error code from errno().

```
int swtd_close(int fd)
```

Description

Close the file handle.

Input

int fd - the file handle from swtd_open() return value.

Output

OK will be zero.

The other has some error, to get error code from errno().

4. Special Note

When you “kill the application with -9” or “kill without option” or “Ctrl+c” the kernel will change to auto ack the sWatchDog.

When your application enables the sWatchDog and does not ack, your application may have a logical error, or your application has made a core dump. The kernel will not change to auto ack. This can cause a serious problem, causing your system to reboot again and again.

5. User application example

Example 1:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <moxadevice.h>

int main(int argc, char *argv[])
{
    int fd;

    fd = swtd_open();
    if ( fd < 0 ) {
        printf("Open sWatchDog device fail !\n");
        exit(1);
    }
    swtd_enable(fd, 5000); // enable it and set it 5 seconds
    while ( 1 ) {
        // do user application want to do
        ....
        ....
        swtd_ack(fd);
        ....
        ....
    }
    swtd_close(fd);
    exit(0);
}
```

```
}
```

The makefile is shown below:

```
all:
    arm-linux-gcc -o xxxx xxxx.c -lmoxalib
```

Example 2:

```
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <string.h>
#include <sys/stat.h>
#include <sys/ioctl.h>
#include <sys/select.h>
#include <sys/time.h>
#include <moxadevice.h>

static void mydelay(unsigned long msec)
{
    struct timeval time;

    time.tv_sec = msec / 1000;
    time.tv_usec = (msec % 1000) * 1000;
    select(1, NULL, NULL, NULL, &time);
}

static int swtdfd;
static int stopflag=0;

static void stop_swatcdog()
{
    stopflag = 1;
}

static void do_swatcdog(void)
{
    swtd_enable(swtdfd, 500);
    while ( stopflag == 0 ) {
        mydelay(250);
        swtd_ack(swtdfd);
    }
    swtd_disable(swtdfd);
}

int main(int argc, char *argv[])
{
    pid_t sonpid;

    signal(SIGUSR1, stop_swatcdog);
    swtdfd = swtd_open();
    if ( swtdfd < 0 ) {
        printf("Open sWatchDog device fail !\n");
        exit(1);
    }
    if ( (sonpid=fork()) == 0 )
        do_swatcdog();
    // do user application main function
    ....
    ....
    ....
    // end user application
    kill(sonpid, SIGUSR1);
    swtd_close(swtdfd);
    exit(1);
}
```

The makefile is shown below:

```
all:
    arm-linux-gcc -o xxxx xxxx.c -lmoxalib
```

UART

The normal tty device node is located at `/dev/ttyM0 ... ttyM3`.

The W311/321/341 support Linux standard termios control. The Moxa UART Device API allows you to configure ttyM0 to ttyM3 as RS-232, RS-422, 4-wire RS-485, or 2-wire RS-485. The W311/321/341 support RS-232, RS-422, 2-wire RS-485, and 4-wire RS485.

You must include `<moxadevice.h>`.

```
#define RS232_MODE    0
#define RS485_2WIRE_MODE 1
#define RS422_MODE    2
#define RS485_4WIRE_MODE 3
```

1. Function: MOXA_SET_OP_MODE

```
int ioctl(fd, MOXA_SET_OP_MODE, &mode)
```

Description

Set the interface mode. Argument 3 mode will pass to the UART device driver and change it.

2. Function: MOXA_GET_OP_MODE

```
int ioctl(fd, MOXA_GET_OP_MODE, &mode)
```

Description

Get the interface mode. Argument 3 mode will return the interface mode.

There are two Moxa private ioctl commands for setting up special baudrates.

Function: MOXA_SET_SPECIAL_BAUD_RATE

Function: MOXA_GET_SPECIAL_BAUD_RATE

If you use this ioctl to set a special baudrate, the termios cflag will be B4000000, in which case the B4000000 define will be different. If the baudrate you get from termios (or from calling tcgetattr()) is B4000000, you must call ioctl with MOXA_GET_SPECIAL_BAUD_RATE to get the actual baudrate.

Example to set the baudrate

```
#include <moxadevice.h>
#include <termios.h>
struct termios term;
int fd, speed;
fd = open("/dev/ttyM0", O_RDWR);
tcgetattr(fd, &term);
term.c_cflag &= ~(CBAUD | CBAUDEX);
term.c_cflag |= B4000000;
tcsetattr(fd, TCSANOW, &term);
speed = 500000;
ioctl(fd, MOXA_SET_SPECIAL_BAUD_RATE, &speed);
```

Example to get the baudrate

```
#include <moxadevice.h>
#include <termios.h>
struct termios term;
int fd, speed;
fd = open("/dev/ttyM0", O_RDWR);
tcgetattr(fd, &term);
```

```
if ( (term.c_cflag & (CBAUD|CBAUDEX)) != B4000000 ) {  
    // follow the standard termios baud rate define  
} else {  
    ioctl(fd, MOXA_GET_SPECIAL_BAUD_RATE, &speed);  
}
```

Baudrate inaccuracy

Divisor = 921600/Target Baud Rate. (Only Integer part)

ENUM = 8 * (921600/Target - Divisor) (Round up or down)

Inaccuracy = (Target Baud Rate – 921600/(Divisor + (ENUM/8))) * 100%

E.g.,

To calculate 500000 bps

Divisor = 1, ENUM = 7,

Inaccuracy = 1.7%

*The Inaccuracy should less than 2% for work reliably.

Special Note

1. If the target baudrate is not a special baudrate (e.g. 50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600), the termios cflag will be set to the same flag.
2. If you use stty to get the serial information, you will get speed equal to 0.

DO

Using Dout pin 22 to control Dout close nad open , if make Pin 22 pull high being closed and Pin22 pull low being open.

Usage like:

echo "22 1 1" > /proc/driver/dio → The Do will be open

echo "22 1 0" > /proc/driver/dio → The Do will be close

“Software Lock” is an innovative technology developed by the Moxa engineering team. It can be adopted by a system integrator or developer to protect his applications from being copied. An application is compiled into a binary format bound to the embedded computer and the operating system (OS) that the application runs on. As long as one obtains it from the computer, he/she can install it into the same hardware and the same operating system. The add-on value created by the developer is thus lost.

Moxa’s engineering used data encryption to develop this protection mechanism for your applications. The binary file associated with each of your applications needs to undergo an additional encryption process after you have developed it. The process requires you to install an encryption key in the target computer.

1. Choose an encryption key (e.g., “ABigKey”) and install it in the target computer by a pre-utility program, ‘setkey’.

#setkey ABigKey

Note: set an empty string to clear the encryption key in the target computer by:

#setkey “““

2. Develop and compile your program in the development PC.
3. In the development PC, run the utility program ‘binencryptor’ to encrypt your program with an encryption key.

#binencryptor yourProgram ABigKey

4. Upload the encrypted program file to the target computer by FTP or NFS and test the program.

The encryption key is a computer-wise key. That is to say, a computer has only one key installed. Running the program ‘setkey’ multiple times overrides the existing key.

To prove the effectiveness of this software protection mechanism, prepare a target computer that has not been installed an encryption key or install a key different from that used to encrypt your program. In any case, the encrypted program fails immediately.

This mechanism also allows the computer with an encryption key to bypass programs that are not encrypted. Therefore, in the development phase, you can develop your programs and test them in the target computer cleanly.

UC Finder comes in handy if you forget the IP address of the target computer while you have a demand for troubleshooting field problems. This utility works by sending a broadcast message over the LAN to search for IP addresses of target computers. Two versions of UC Finder are provided. The GUI version works in Windows environments, and the command line utility works in Linux environments.

The following topics are covered in this chapter:

- ❑ **Windows UC Finder**
 - Installing the Software
 - Broadcast Search
- ❑ **Linux ufinder**

Windows UC Finder

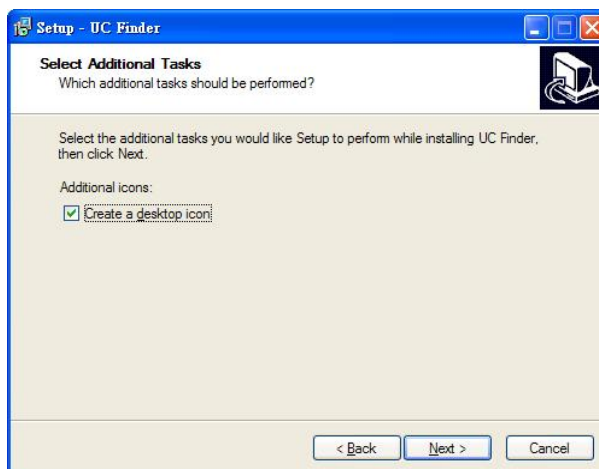
The **UC Finder** utility is used to search the LAN or intranet for Moxa embedded computers.

Installing the Software

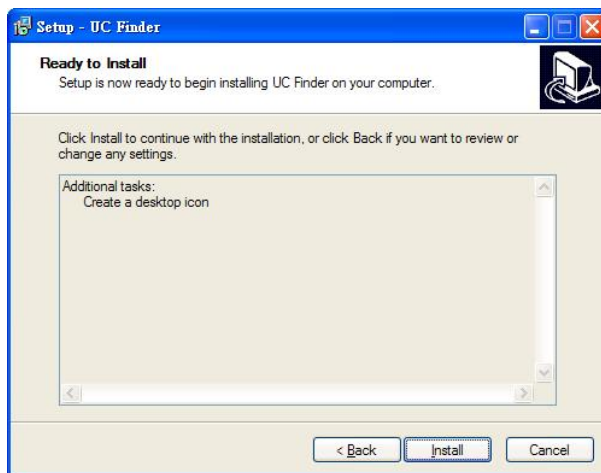
1. Once the Setup program starts running, click on **Next** to proceed.



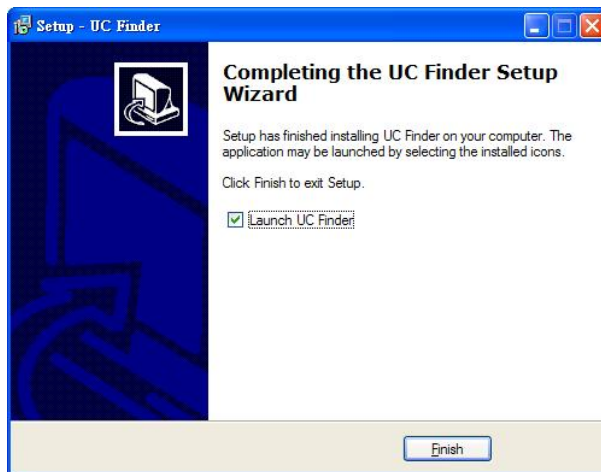
2. Click on **Next** when the **Select Additional Tools** window opens to proceed with the installation.



3. Click on **Next** to install program files in the default directory, or select an alternative location.



4. Click on **Finish** to complete the installation of UC Finder.

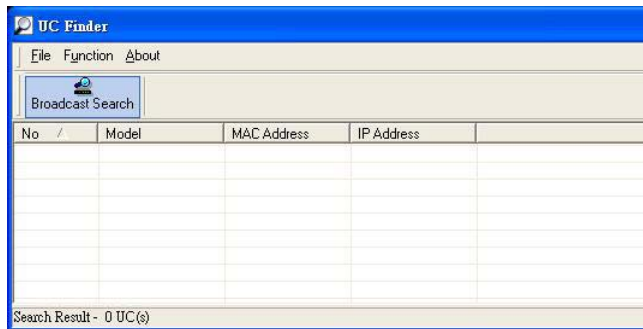


Broadcast Search

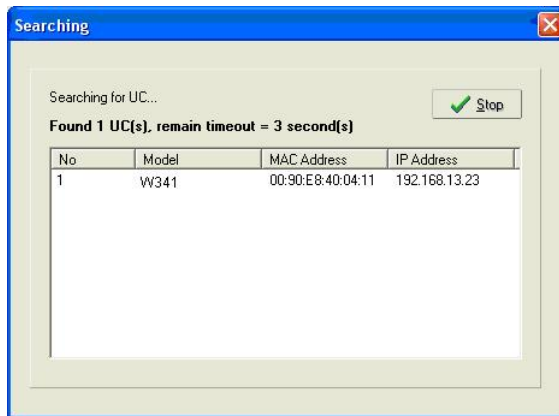
The **Broadcast Search** function is used to locate all W311/321/341 units that are connected to the same LAN as your Windows computer.

Since the Broadcast Search function searches by MAC address and not IP address, all W311/321/341's connected to the LAN will be found, regardless of whether or not they are on the same subnet as the host.

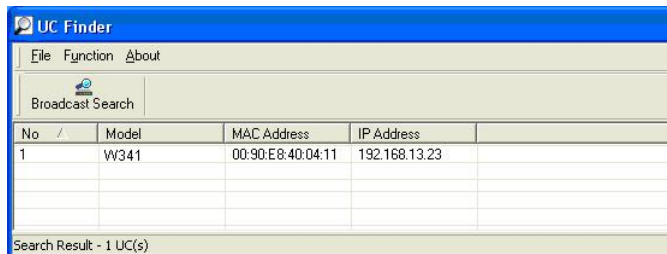
1. Click on the **Broadcast Search** button to start searching.



2. The **Searching** window displays the **Model**, **MAC Address**, and **IP Address** of devices that were located..



3. When the search is complete, the same information is displayed in the UC Finder window.



NOTE UC Finder is designed to determine the IP addresses of all UC units connected to the same LAN the host that is running UC Finder. To configure UC's IP addresses or other configuration parameters, use Telnet over the network, or connect directly to the serial Console port to access the W311/321/341's Console utility.

Linux ucfinder

Copy **ucfinder** from the Documentation and Software CD to your Linux PC, and then use the following command to start the program. UC Finder will automatically locate all W311/321/341 units on the LAN, and then report their IP addresses.

```
#./ucfinder
```

A

System Commands

busybox (V0.60.4): Linux normal command utility collection

File manager

- | | |
|-----------|---|
| 1. cp | copy file |
| 2. ls | list file |
| 3. ln | make symbolic link file |
| 4. mount | mount and check file system |
| 5. rm | delete file |
| 6. chmod | change file owner & group & user |
| 7. chown | change file owner |
| 8. chgrp | change file group |
| 9. sync | sync file system, let system file buffer be saved to hardware |
| 10. mv | move file |
| 11. pwd | display now file directly |
| 12. df | list now file system space |
| 13. mkdir | make new directory |
| 14. rmdir | delete directory |

Editor

- | | |
|----------|---------------------------|
| 1. vi | text editor |
| 2. cat | dump file context |
| 3. zcat | compress or expand files |
| 4. grep | search string on file |
| 5. cut | get string on file |
| 6. find | find file where are there |
| 7. more | dump file by one page |
| 8. test | test file exist or not |
| 9. sleep | sleep (seconds) |
| 10. echo | echo string |

Network

- | | |
|--------------|------------------------|
| 1. ping | ping to test network |
| 2. route | routing table manager |
| 3. netstat | display network status |
| 4. ifconfig | set network ip address |
| 5. tracerout | trace route |
| 6. tftp | |
| 7. telnet | |
| 8. ftp | |

Process

1. **kill** **kill process**
2. **ps** **display now running process**

Other

1. **dmesg** **dump kernel log message**
2. **stty** **to set serial port**
3. **zcat** **dump .gz file context**
4. **mknod** **make device node**
5. **free** **display system memory usage**
6. **date** **print or set the system date and time**
7. **env** **run a program in a modified environment**
8. **clear** **clear the terminal screen**
9. **reboot** **reboot / power off/on the server**
10. **halt** **halt the server**
11. **du** **estimate file space usage**
12. **gzip, gunzip** **compress or expand files**
13. **hostname** **show system's host name**

MOXA special utilities

1. **backupfs** **backup file system (user directory)**
2. **bf** **built the file system (user directory)**
3. **kversion** **show kernel version**
4. **cat /etc/version** **show user directory version**
5. **upramdisk** **mount ramdisk**
6. **downramdisk** **unmount ramdisk**

B

Service Information

This appendix shows you how to contact Moxa for information about this and other products, and how to report problems.

The following topics are covered in this appendix:

- MOXA Internet Services**
- Problem Report Form**
- Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....support@moxa.com

World Wide Web (WWW) Site for product information:

.....<http://www.moxa.com>

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- ◆ Provide evidence of original purchase.
- ◆ Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- ◆ Fill out the Problem Report Form (PRF). Include as much detail as possible for a shorter product repair time.
- ◆ Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>