

IPCop v1.4.0 Installation Manual

**Pete Walker
Harry Goldschmitt
Stephen Pielschmidt**

IPCop v1.4.0 Installation Manual

by Pete Walker, Harry Goldschmitt, and Stephen Pielschmidt

Copyright © 2002-2004 Peter Walker, Harry Goldschmitt, Stephen Pielschmidt

IPCop is distributed under the terms of the GNU General Public License [<http://www.gnu.org/licenses/gpl.html>].

This software is supplied AS IS. IPCop disclaims all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. IPCop assumes no liability for damages, direct or consequential, which may result from the use of this software.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is included in the section entitled GNU Free Documentation License.

Table of Contents

Introduction	vi
1. Features	vi
2. Overview	vii
1. Preparing to install	1
1.1. Upgrading from IPCop 1.2.0 or Greater	1
1.2. Decide On Your Configuration	1
1.2.1. Network Interfaces	1
1.2.2. Network Configurations	4
1.2.3. Network Configuration Types	4
1.2.4. Connecting to the Internet or External Network	5
1.2.5. Decide On Your Local Network Address(es)	5
1.3. Gather information on Your Hardware	6
1.4. Prepare the IPCop PC	6
1.5. Decide Upon and Prepare the Installation Media	7
1.5.1. Creating the CD	7
1.5.2. Mounting the ISO Image	7
1.5.3. Creating Floppy Disks From Images	8
1.5.4. Making The Installation File Available	8
2. Booting the IPCop Installation Media	10
2.1. Installing From Bootable CD or Bootable Floppy and CD	10
2.2. Installing From Floppy and Web Server or FTP	18
3. Initial Configuration	28
4. After Installation	41
4.1. Choose Your Default Kernel Configuration	41
4.1.1. Changing the Default Configuration	42
4.2. Test Your Access to IPCop	42
4.3. Optionally, Remove Unneeded Hardware	43
A. Quick Home Networking Overview	44
A.1. Wiring	44
A.1.1. Only one computer on GREEN, BLUE or ORANGE	44
A.1.2. Multiple Computer Networks	44
A.2. IP Addressing	44
A.2.1. Format of an Address	44
A.2.2. Networks	44
A.2.3. Network Address Classes	45
A.2.4. Private Address Ranges	45
B. Troubleshooting During The Install	46
B.1. Hidden Console Screens	46
B.2. Loss of the Root Password	47
C. Creating Flash Based IPCop Systems	49
C.1. Why Run a Flash Based System?	49
C.2. Other CF Resources	49
C.3. Task Overview	49
C.4. CF Installation Steps	50
C.4.1. Obtain the Target Machine	50
C.4.2. Install IPCop On a Staging Machine	50
C.4.3. Get mkflash.sh and Associated Files	50
C.4.4. Upload mkflash.sh	50
C.4.5. Run mkflash.sh	51
C.4.6. Write the Compact Flash	51
C.4.7. Install Your New Image and Boot	52
C.4.8. Run the Setup Command	52

C.5. Backing Up Your Compact Flash Using ssh	52
D. GNU Free Documentation License	53
D.1. 0. Preamble	53
D.2. 1. Applicability and Definitions	53
D.3. 2. Verbatim Copying	54
D.4. 3. Copying In Quantity	54
D.5. 4. Modifications	55
D.6. 5. Combining Documents	56
D.7. 6. Collections of Documents	56
D.8. 7. Aggregation With Independent Works	57
D.9. 8. Translation	57
D.10. 9. Termination	57
D.11. 10. Future Revisions of This License	57
D.12. ADDENDUM: How to use this License for your documents	57

List of Tables

1.1. NIC Requirements 3
1.2. Media required for different installation methods 7

Introduction

IPCop Linux is a complete Linux Distribution. Its sole purpose in life is to protect the network that it is installed on. By implementing existing technology, outstanding new technology and secure programming practices, IPCop is the Linux Distribution for those wanting to keep their computers/networks safe and sound.

IPCop is open source and is distributed under the GNU General Public License [<http://www.gnu.org/licenses/gpl.html>]. In addition to the many obvious advantages of open source, the fact that the source is open allows security experts, worldwide, to audit and fix security holes.

It will run on older “rescued” PCs retrieved from the junk heap. For further information on IPCop’s hardware requirements please see the IPCop Hardware Compatibility List [<http://ipcop.sourceforge.net/cgi-bin/twiki/view/PCop/PCopHCLv01>].

1. Features

- A secure, stable and highly configurable Linux based firewall
- Easy administration through the built in web server
- A DHCP client that allows IPCop to, optionally, obtain its IP address from your ISP
- A DHCP server that can help configure machines on your internal network
- A caching DNS proxy, to help speed up Domain Name queries
- A web caching proxy, to speed up web access
- An intrusion detection system to detect external attacks on your network
- The ability to partition your network into a GREEN, safe, network protected from the Internet, a BLUE network for your wireless LAN and a DMZ or ORANGE network containing publicly accessible servers, partially protected from the Internet
- A VPN facility that allows you to connect your internal network to another network across the Internet, forming a single logical network or to securely connect PCs on your BLUE, wireless, network to the wired GREEN network
- Traffic shaping capabilities to give highest priority to interactive services such as ssh and telnet, high priority to web browsing, and lower priority to bulk services such as FTP.
- Improved VPN support with x509 certificates.
- Built from the ground up with ProPolice [<http://www.research.ibm.com/tr1/projects/security/ssp/>] to prevent stack smashing attacks in all applications.
- A choice of four kernel configurations, allowing you to choose an optimum configuration for your circumstances.

An appendix of this manual discusses running IPCop from a flash disk.

2. Overview

You will be installing an operating system on the IPCop PC. It is a Linux based operating system, but it is not meant to be a general-purpose system. The firewall design attempts to eliminate as many features from the system as possible. The central idea is that the more code that runs on the firewall, the more places there are that are vulnerable to attacks. Do not expect facilities like sendmail or FTP daemons to be present. These are not needed on a firewall and may contain holes that are known to malicious users.

Although these instructions will appear to be long and often detailed, take heart. Once you've figured out what you want to do and have obtained your current configuration parameters, installing IPCop will take as little as fifteen minutes.

You will have to boot from the installation media or a floppy. The installation media is distributed as an ISO file. If you have a CD burner, you will probably want to create a bootable CD from the ISO file. If you cannot burn a CD, you will have to place files from the ISO image on a web or FTP server. If the IPCop PC cannot boot from CD, you will have to create a bootable floppy.

Chapter 1. Preparing to install



CAUTION: When you install IPCop on a PC, the hard drive will be formatted and all data on it will be lost.

1.1. Upgrading from IPCop 1.2.0 or Greater

Starting with IPCop 1.3.0, you can upgrade your IPCop PC from IPCop 1.2.0 or later and save your configuration. Use the web interface to log in to your IPCop PC and take a backup on a floppy, using the Backup Administrative web page. If you don't know how to do this, please read the IPCop Administration Manual section entitled System->Backup AW [<http://www.ipcop.org/1.3.0/en/admin/html/system.html#backup>]. During installation you will be asked whether you wish to restore your settings from a backup floppy. Insert the backup floppy in your floppy disk drive and respond, "Restore".

1.2. Decide On Your Configuration

1.2.1. Network Interfaces

IPCop defines up to four network interfaces, RED, GREEN, BLUE and ORANGE.

1.2.1.1. RED Network Interface

This network is the Internet or other untrusted network. IPCop's primary purpose is to protect the GREEN, BLUE and ORANGE networks and their computers from traffic originating on the RED network. Your current connection method and hardware are used to connect to this network.

1.2.1.2. GREEN Network Interface

This interface only connects to the computer(s) that IPCop is protecting. It is presumed to be local. Traffic to it is routed though an Ethernet NIC on the IPCop computer firewall.

1.2.1.3. BLUE Network Interface

This optional network allows you to place wireless devices on a separate network. Computers on this network cannot get to the GREEN network except tightly controlled “pinholes”, or via a VPN. Traffic to this network is routed through an Ethernet NIC.

1.2.1.4. ORANGE Network Interface

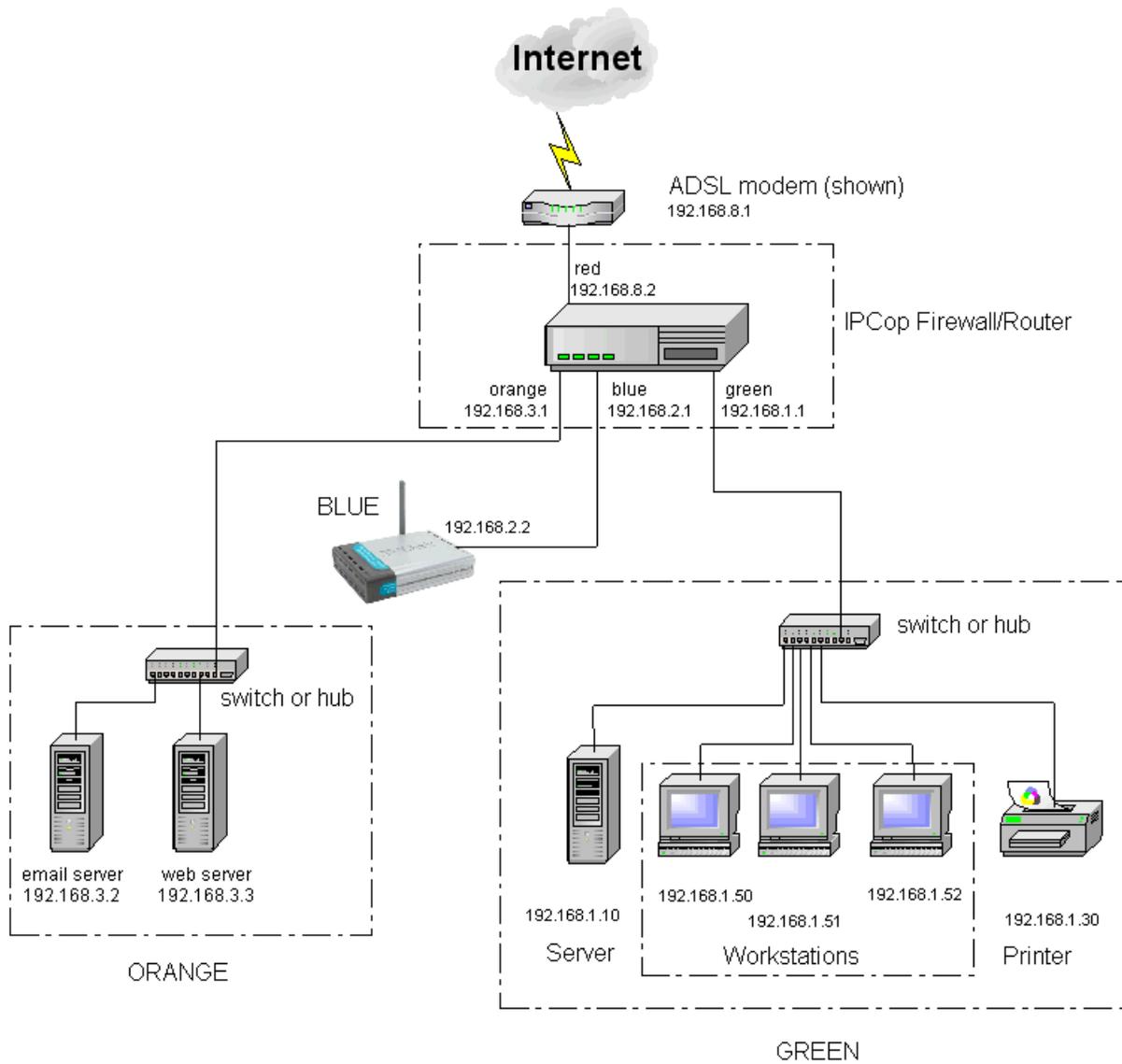
This optional network allows you to place publicly accessible servers on a separate network. Computers on this network cannot get to the GREEN or BLUE networks, except through tightly controlled “DMZ pinholes”. Traffic to this network is routed through an Ethernet NIC.

1.2.1.5. Network Interfaces

Your firewall will need at least 1 Ethernet cable and network interface card (NIC). It may need up to 4 NICs, depending on the network configuration you choose and your connection to the Internet.

All NICs must be different physical cards (or their equivalent if you have multport cards).

Ignoring for a moment the RED network, you will have to plug a separate Ethernet NIC and cable into your firewall for each of the GREEN, BLUE and/or ORANGE network. The GREEN and RED networks are required. The ORANGE and BLUE networks are optional. The interface requirements for your RED network will vary depending on your connection to the Internet. The RED network may require an additional Ethernet card and cable.



RED, ORANGE, BLUE, GREEN Configuration

The RED, ORANGE, BLUE, GREEN diagram shows that, other than the RED net, each of the networks needs an Ethernet card. If you are currently using an Ethernet connection to the Internet, you will need a card for it, too. The networks must have different network addresses.

Note

Remember, the BLUE and ORANGE networks are optional.

Table 1.1. NIC Requirements

Connection	Modem	ISDN	USB ADSL	Ethernet
RED, GREEN	1 NIC (G)	1 NIC (G)	1 NIC (G)	2 NICs (G,R)
RED, BLUE, GREEN	2 NICs (B,G)	2 NICs (B,G)	2 NICs (B,G)	3 NICs (B,G,R)
RED, ORANGE, GREEN	2 NICs (O,G)	2 NICs (O,G)	2 NICs (O,G)	3 NICs (O,G,R)
RED, ORANGE, BLUE, GREEN	3 NICs (O,B,G)	3 NICs (O,B,G)	3 NICs (O,B,G)	4 NICs (O,B,G,R)

1.2.1.6. Relative Security of IPCop Network Interfaces

The security model of IPCop is that the GREEN network is fully trusted and any requests from this network, whether initiated by a user or by a machine infected with a virus, Trojan horse or other “malware” is legitimate and allowed by IPCop.

A new feature of IPCop 1.4.0, allows for the Intrusion Detection System to be enabled for each network interface. It is always a good idea to glance at the IDS logs for your internal networks to see if a machine on your network is behaving strangely. This may indicate a virus infection.

The order of trustworthiness of networks in order of increasing trust is:

RED → ORANGE → BLUE → GREEN

1.2.2. Network Configurations

The base configuration is RED/GREEN where IPCop protects a single internal network from the Internet. If you have a wireless access point then you can attach it to the BLUE NIC and configure IPCop to restrict the access of machines on your wireless LAN. If you have some servers that need to be accessible to the Internet you can place them in an untrusted DMZ attached to the ORANGE NIC. You should decide which combination you want for your site.

1.2.3. Network Configuration Types

Since the RED interface can connect either by modem or by Ethernet, there are eight Network Configuration Types:

- GREEN (RED is modem/ISDN)
- GREEN + RED (RED is Ethernet)
- GREEN + ORANGE + RED (RED is Ethernet)
- GREEN + ORANGE (RED is modem/ISDN)
- GREEN + BLUE + RED (RED is Ethernet)
- GREEN + BLUE (RED is modem/ISDN)
- GREEN + BLUE + ORANGE + RED (RED is Ethernet)
- GREEN + BLUE + ORANGE (RED is modem/ISDN)

1.2.4. Connecting to the Internet or External Network

How are you currently connecting to the Internet, today?

If you are connected through an external broadband modem or router, you probably will be connected via an Ethernet network interface card or NIC. In any case, a similar card must be in your IPCop PC. If you are connected via an internal analog modem, ISDN modem, or ADSL USB modem, this must be moved to the IPCop PC. If you are connected via an external dial up modem, you will have to connect it to your IPCop PC.

This hardware will be used for your RED network interface.

Write down some key parameters from your current interface.

- Check how you are currently obtaining your IP address: static, DHCP, PPPOE or PPTP.
- If you obtain your IP address via DHCP, check to see if your system has a hostname it is providing to your ISP's DHCP server, see [Checking Your DHCP Host Name](#), below.
- Check what your name servers' addresses are. Your ISP's DHCP server may provide the addresses automatically or you may need to enter them manually.
- Note any default sub domain addresses specified. These allow you to specify hosts like mail or news without entering the full host name, see the discussion in DHCP setup, below.

1.2.4.1. Checking Your DHCP Host Name

If you don't know if your ISP requires a host name, or you don't know what it is, check the paperwork that came with your ISP's installation kit or call their support center for help. If that fails, enter:

```
$ ifconfig -a
```

on a *nix platform, and look at your eth0 IP address. On Windows 95, 98, ME, etc. the command is

```
C:\winipcfg
```

entered from the command prompt. On Windows NT and Windows 2000, the command is

```
C:\ipconfig /all
```

In any case, write down your IP address and then issue an

```
$ nslookup nnn.nnn.nnn.nnn
```

command, where *nnn.nnn.nnn.nnn* is your IP address. If you get a response, write down the full host name you receive. The first part may be your DHCP hostname, the last part may be used to configure IPCop's DHCP server.

1.2.5. Decide On Your Local Network Address(es)

Decide what your GREEN or local network address range will be. This is not the IP address provided by your ISP. Addresses on this interface will never appear on the Internet. IPCop uses a technique called Port Address Translation, PAT, to hide your GREEN machines from outside eyes. To make sure there are no IP address conflicts, it is suggested that you choose one of the address ranges defined in RFC1918 [<ftp://ftp.isi.edu/in-notes/rfc1918.txt>] as private (non-routable) addresses. There are over 65,000 of these network address ranges you can choose from. For a list of available network address ranges, please see Appendix A . The easiest network to pick is the 192.168.1.xxx network. This will allow IPCop to handle over 250 computers. Typically routers and firewalls are placed at the top or bottom of the address range, so we suggest that you pick 192.168.1.1 for your GREEN network interface. IPCop will automatically set your network mask based on your IP address, but you can modify it, if you need to.

If you will be using BLUE and/or ORANGE networks pick different network addresses for each of them. For example, BLUE might be 192.168.2.xxx and ORANGE might be 192.168.3.xxx. This will allow over 250 computers on each network.

1.3. Gather information on Your Hardware

Although IPCop will automatically probe your machine for NICs, it may be necessary to input individual NIC card's configuration parameters during installation. In this case the type, IO address and IRQ number will be needed. The easiest way to configure the cards or determine this information is via a program on the floppy disk that comes with the NIC. Alternatively, check the manufacturer's web site.

If you have an internal ISDN modem, IPCop will automatically probe it, too. Again, if IPCop can't determine the modem information, you will need to know the type, IO address and IRQ number of your modem. The easiest way to configure the modem or determine this information is via a program on the floppy disk that came with the card. Alternatively, check the manufacturer's web site. In addition, you will have to know the country and protocol of the connection, as well as the local phone number for your modem.

1.4. Prepare the IPCop PC

Obtain the IPCop PC. Check the IPCop Hardware Compatibility List [<http://ipcop.sourceforge.net/cgi-bin/twiki/view/IPCop/IPCopHCLv01>] to verify the PC you are planning to use will support IPCop.

Insert any additional network cards needed to handle your configuration in the IPCop PC. You will need an Ethernet NIC for the GREEN interface. If you decide on a BLUE or ORANGE interface, you will need an extra NIC for each. If your RED interface is via Ethernet you will need one Ethernet NIC for this network, as well.

Insert the ISDN modem card, if needed.

During the installation process a video monitor will need to be attached to the IPCop PC. IPCop stays in character mode, so almost any monitor will do. The monitor can be removed after the install. In addition, a keyboard will be needed. If your BIOS keyboard test can be disabled, the keyboard can also be removed after the installation.

Set the BIOS parameters so that the target machine will operate, as much as possible, as a stand-alone server. For example:

- Turn off the CPU power saver feature; the target computer must wake on all network activity on all NICs and/or modems. It's usually easier and safer to just turn off the power saver features. You can leave the video power saver turned on.
- Set the BIOS to boot on power up.

- Turn off the BIOS keyboard test, if possible.
- Set the power state to “Always restore power after power failure”. This will guarantee your IPCop PC will power up and reboot after power is restored.
- IPCop can backup your configuration to a floppy disk drive. It is not uncommon for the floppy to be accidentally left in the floppy drive.

If you are installing from CD drive, make sure your system will only boot from the CD drive and hard drive. Turn off all types of boot, except your hard drive after installation completes.

1.5. Decide Upon and Prepare the Installation Media

Obtain an ISO image from www.ipcop.org [<http://www.ipcop.org/>]. The size of this image is about 37 megabytes. You should check the MD5 checksum [http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopFAQ#What_is_this_big_md5_number_all_] of the file you downloaded against the one on the IPCop web site before going any further.

There are three possible ways to install IPCop. The following table summarizes the requirements for each.

Table 1.2. Media required for different installation methods

Method	Boot Floppy	Driver Floppy	CD Drive	FTP/Web Server
Bootable CD	N	N	Y	N
Bootable Floppy with CD	Y	N	Y	N
Bootable Floppy with FTP/Web Server	Y	Y	N	Y

If the IPCop PC has a CD drive and its BIOS can boot from CD, you can use the “Bootable CD” media for the install. The CD drive can be removed after the install.

If the IPCop PC cannot boot from CD, but has both a floppy drive and a CD drive, the “Bootable Floppy With CD” can be used. Both the floppy drive and CD drive can be removed after the install. However, if you plan on using IPCop’s backup and restore facilities, you may want to keep the floppy disk in the IPCop PC.

Finally, if the IPCop PC has only a floppy drive or you do not own a CD burner, the “Bootable Floppy with FTP/Web Server” must be used. Again, the floppy drive can be removed after the install. Again, if you plan on using IPCop’s backup and restore facilities, you may want to keep the floppy drive in the IPCop PC.

1.5.1. Creating the CD

If you have a CD burner, use your favorite CD writer package to transfer the ISO image to a CD-ROM. Be aware that the IPCop CD image is a full CD image. In many CD writer software packages, it can be difficult to find the “Burn CD From ISO or Disk Image” option. The option may not be placed under the obvious menu. If you wind up with only one file on the CD, you have not created the CD correctly.

1.5.2. Mounting the ISO Image

If you don’t have a CD writer, have no fear. You can still install IPCop, but you will have to go through some extra work. What has to be done depends upon the hardware and operating systems you have available on other computers.

1.5.2.1. Linux

If you have a Linux or Unix system, you can mount the CD image, using the following commands:

```
# losetup /dev/loop0 /path/to/IPCop/iso
```

where `/path/to/IPCop/iso` is the file name of IPCop's `iso` file. This links a "loop back" hardware level device to the IPCop ISO file.

```
# mount -r -t iso9660 /dev/loop0 /mnt/cdrom
```

This actually mounts the loop back hardware device on a *nix file system. The CD-ROM image will appear at `/mnt/cdrom`. NOTE: On most systems you must have root authority or use the `sudo` command to mount file systems.

1.5.2.2. Windows

There are several utilities such as ISO Buster and WinImage available on the Internet that can be used to open the ISO image. Download one of them, and follow their directions to open the IPCop ISO file.

1.5.2.3. Macintosh

On Macintosh OS X, Apple's Disk Copy utility will open the ISO image. There does not seem to be a free or public domain utility available to open IPCop's ISO images on Mac systems before OS X. However, many commercial CD-ROM burning programs do have this capability. If you have a CD burner, check the software that came with it.

1.5.3. Creating Floppy Disks From Images

If your IPCop PC has a CD-ROM, but your BIOS will not allow a CD-ROM boot, you will need to create a floppy boot disk. If your IPCop PC does not have a CD-ROM, you will need to create both the floppy boot disk and the driver floppy disk. Both images reside in the `/images` directory on the ISO image.

1.5.3.1. Creating Floppies On *nix and Macintosh OS X

On Linux, Unix and Macintosh OS X systems, creating the floppies can be done from a terminal window with the `dd` command:

```
# dd if=/mnt/cdrom/images/boot-1.4.0.img of=/dev/fd0 bs=1k count=1440
```

Use the same command with `if=` pointing to the driver disk image to create the driver floppy, if needed.

1.5.3.2. Creating Floppies on Windows

Two utilities are provided in the `/dosutils` directory on the CD and its ISO image. These are `rawrite.exe` and `rawritewin.exe`. `rawrite.exe` is a DOS based command that can be used to create floppies from the `.img` files in the `/images` directory. Similarly, `rawritewin.exe` is a windows executable that you can run under Windows to create the floppy disks from the disk images on the CD.

1.5.4. Making The Installation File Available

This step is only needed if you are installing from bootable floppy and FTP/Web Server. In the root directory `/` of the ISO image there is a file named `ipcop-1.4.0.tgz`. This file contains a compressed image of the IPCop hard drive. Copy this file to a machine that is running a web server or FTP server. Put it where the server can find it during install. During the install, IPCop will log in to your FTP or web server as anonymous. Most servers do not allow anonymous users to access files out of the server's hierarchy. Even though a directory appears at the top level of the server, such as `/pub` they really are somewhere else, such as `/anonftp/pub`.

If your IPCop PC uses SCSI disk drives then you also need to copy the file `scsidrv-1.4.0.img` from the `/images` folder of the ISO image to this directory.

If you are creating your private network for the first time, change the IP address of the server machine to be on the private, GREEN, network, using a static address. You only need to do this for the duration of the install.

If your server machine is connected to the Internet, remove the connection and physically connect your IPCop PC and other machines together. See Appendix A, for a discussion of your choices. If you are using 192.168.1.1 for the IPCop PC, 192.168.1.2 is a good address for the server. Set the server up with a static IP address, temporarily. You will need to reboot any Windows PC if you change its IP address.

Verify that the IPCop installation file is available via the FTP command or entering its URL from a browser, even if you have to do it from the server machine. You can cancel the download or close your browser once you are sure the URL works.

Chapter 2. Booting the IPCop Installation Media

You are now ready to install IPCop.

Caution

Remember, installing IPCop on a computer will erase its hard drive.

Even though the IPCop installation steps are very similar, each method of installing IPCop will be discussed separately. If you are not sure of which method to choose, see the discussion in the chapter above.

2.1. Installing From Bootable CD or Bootable Floppy and CD

Put the IPCop CD in the IPCop PC's CD-ROM drive. If necessary, put the IPCop bootable floppy in the floppy drive. Press the reset button to start the boot sequence. If the IPCop PC does not boot, check the BIOS boot parameters.

Soon the boot up screen, below, will appear. If it does not appear, check that your monitor is connected to the video port on the target machine, is powered on and that you have booted from the CD or floppy drive.

```
ISOLINUX 2.08 2003-12-12 Copyright (C) 1994-2003 H. Peter Anvin

Welcome to IPCop, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

-----
----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
----
-----

Press RETURN to boot IPCop default installation.

Or, if you are having trouble you can try these options....

Type:  nopcmcia to disable PCMCIA detection
       nousb to disable USB detection
       nousborpcmcia to disable both PCMCIA & USB detection

boot: _
```

This screen contains a warning that all your existing data will be destroyed.

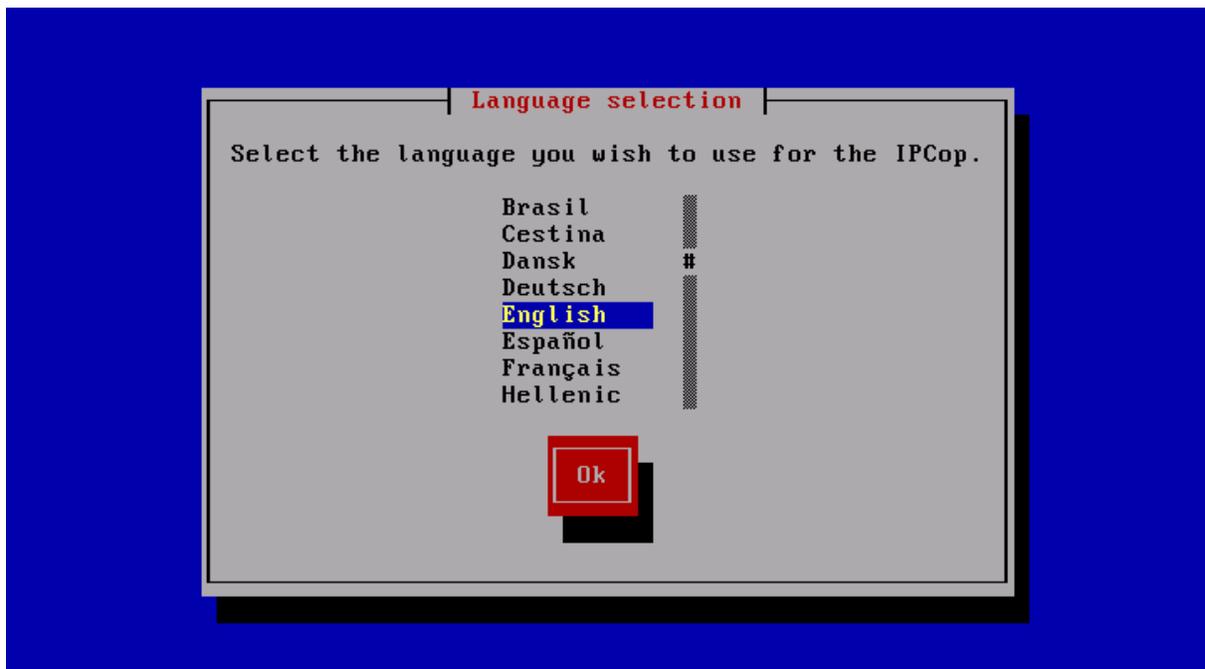
At this point you may just press the **Enter** key, or enter one of the three installation options “nopcmcia”, “nousb” or “nousborpcmcia”. The installation options will restrict the devices that the IPCop installation process detects. Use these options only if the standard installation runs into trouble identifying PCMCIA or USB devices attached to the target machine. You may also eject the IPCop media and reboot to abort the installation.

```
zone(0): 4096 pages.  
zone(1): 61440 pages.  
zone(2): 0 pages.  
Kernel command line: BOOT_IMAGE=vmlinuz ide=nodma initrd=instroot.gz root=/dev/r  
am0 rw  
ide_setup: ide=nodma : Prevented DMA  
Initializing CPU#0  
Detected 1615.700 MHz processor.  
Console: colour UGA+ 80x25  
Calibrating delay loop... 3217.81 BogoMIPS  
Memory: 253900k/262144k available (1142k kernel code, 7792k reserved, 350k data,  
84k init, 0k highmem)  
Dentry cache hash table entries: 32768 (order: 6, 262144 bytes)  
Inode cache hash table entries: 16384 (order: 5, 131072 bytes)  
Mount cache hash table entries: 512 (order: 0, 4096 bytes)  
Buffer cache hash table entries: 16384 (order: 4, 65536 bytes)  
Page-cache hash table entries: 65536 (order: 6, 262144 bytes)  
CPU: Trace cache: 12K uops, L1 D cache: 8K  
CPU: L2 cache: 512K  
Intel machine check architecture supported.  
Intel machine check reporting enabled on CPU#0.  
CPU: Intel(R) Pentium(R) 4 CPU 1.60GHz stepping 08  
Enabling fast FPU save and restore... done.  
Enabling unmasked SIMD FPU exception support... done.  
Checking 'hlt' instruction... _
```

During boot up many kernel informational messages will scroll by.

These can be ignored unless a hardware problem is detected. If an error is detected, the boot may stop.

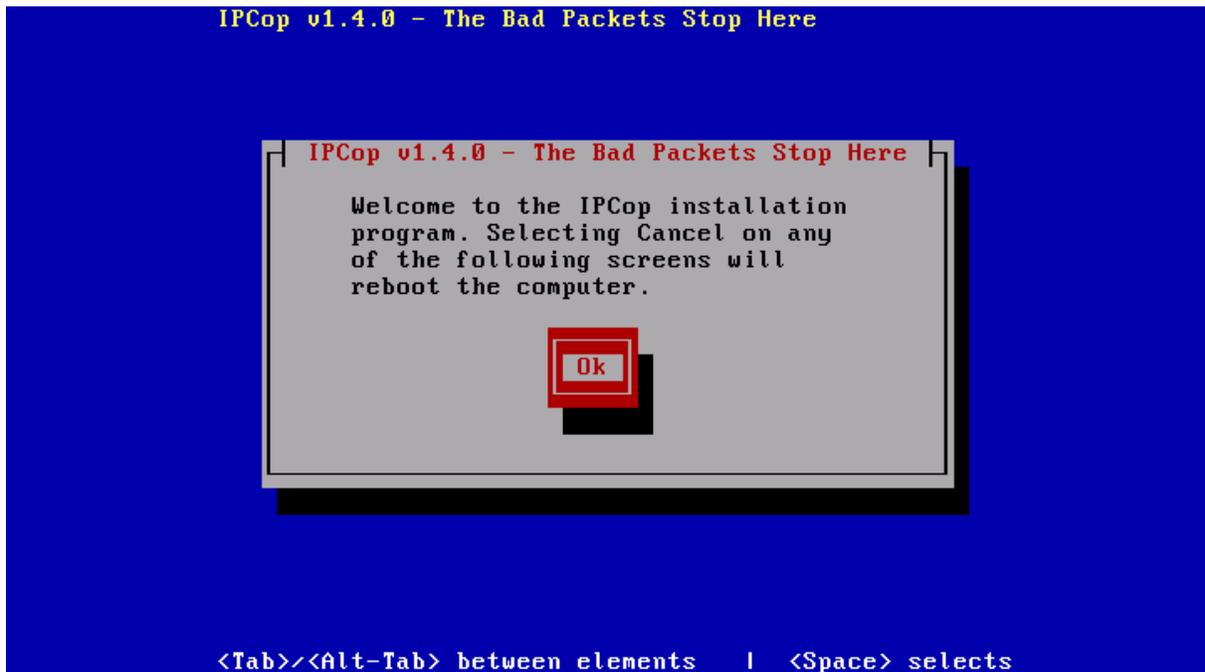
After a few seconds, the language selection screen will appear.



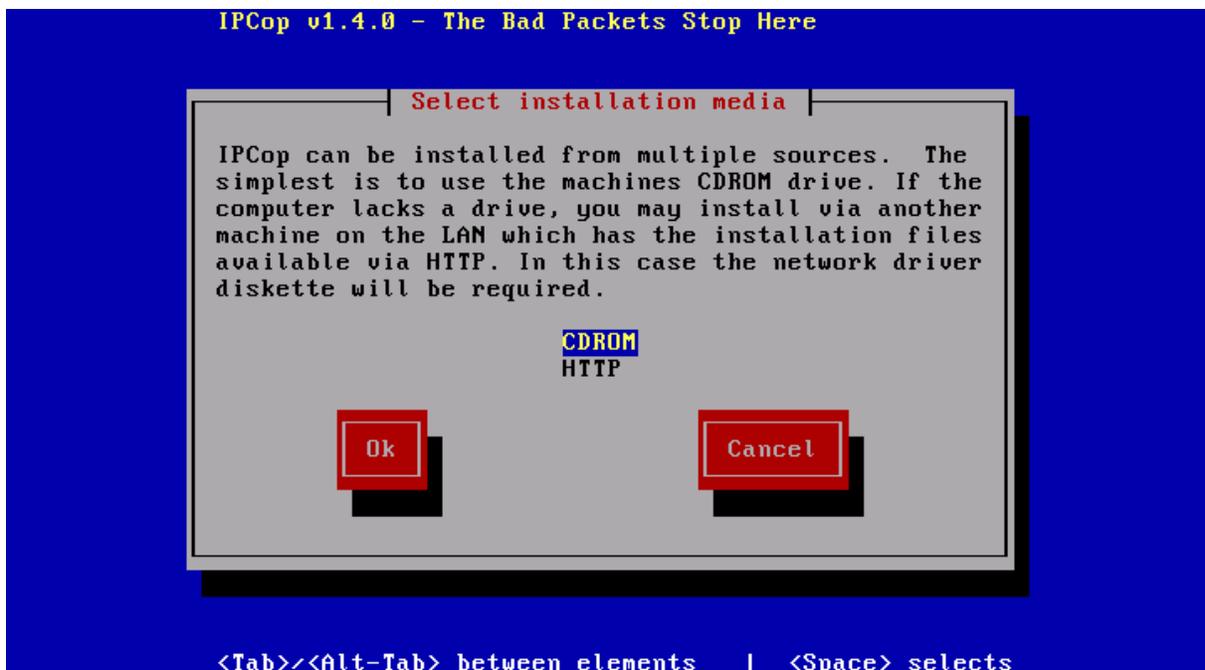
At this time Brazilian Portuguese, Czech, Danish, German, Greek, English, Spanish, French, Hungarian, Italian, Latin American Spanish (Latino), Dutch, Norwegian, Portuguese, Finnish, Swedish, and Turkish are available.

Note: On this and all other installation screens, the mouse is ignored. To move the cursor around the screen, use the **Tab** key and the keyboard arrow keys. To select an item, press the **Space** key. To accept the language choice, press the **Enter** key.

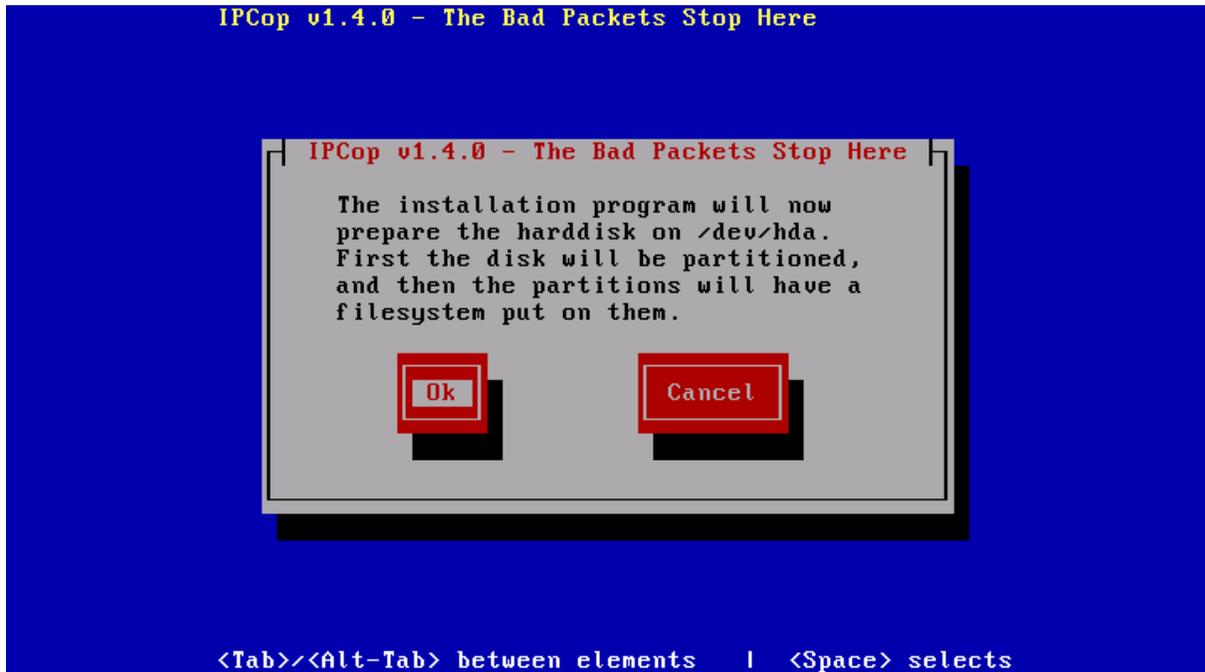
From this point on, in the install, all dialogs, menus and web pages will appear in your chosen language.



The next screen simply informs you of how to abort the installation. " Select the Cancel and press the **Enter** key. "

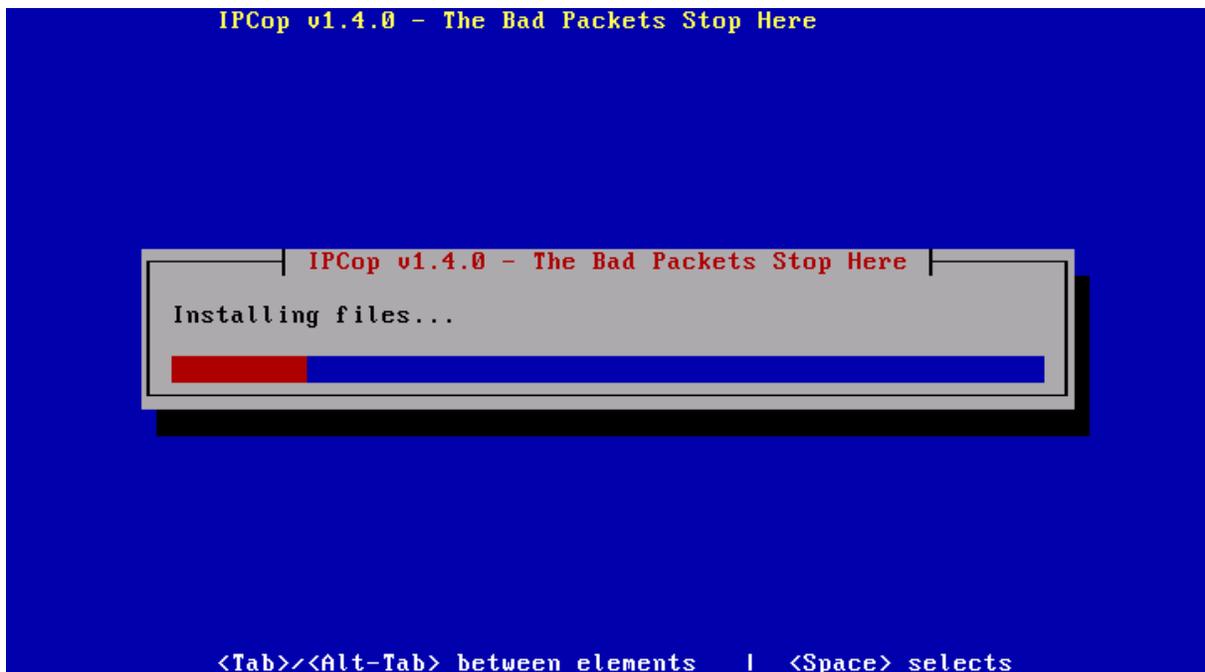


The next dialog box lets you choose the installation media. Since you are installing from CD-ROM, select it, tab to the Ok button and press the **Enter** key.

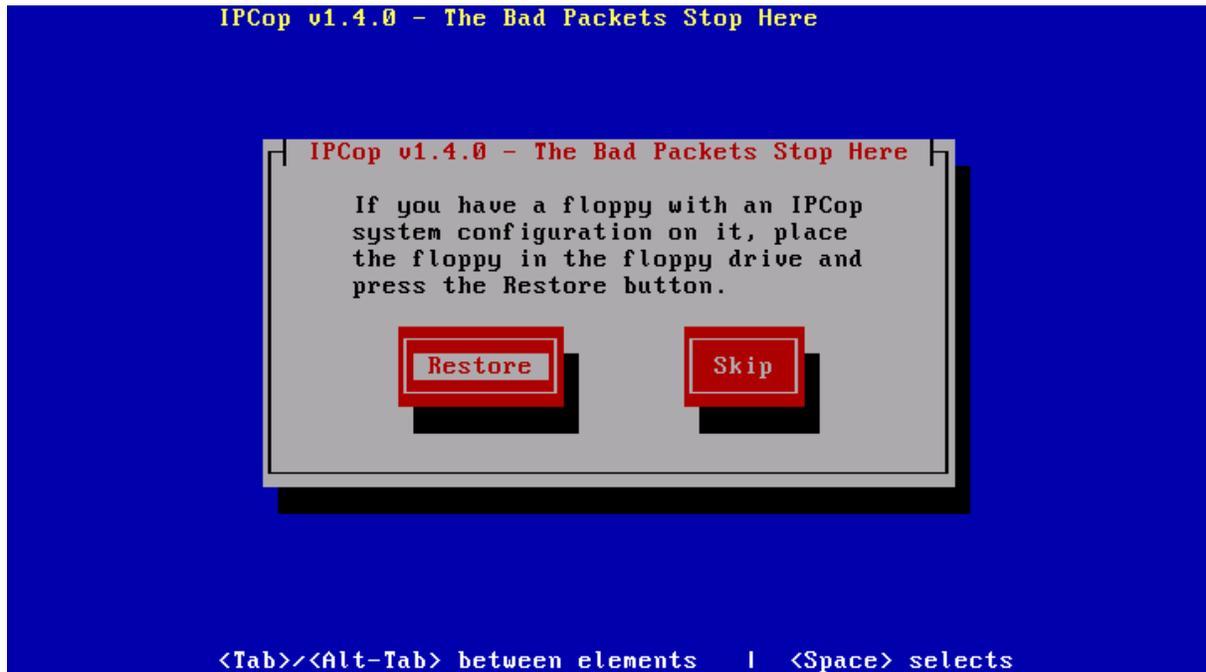


Your final warning appears next.

After you select Ok and press **Enter** on this screen all of the data on your hard drive will be erased. To abort the installation, select Cancel and press the **Enter** key.



Next IPCop will format and partition your hard drive. Then it will install all its files.



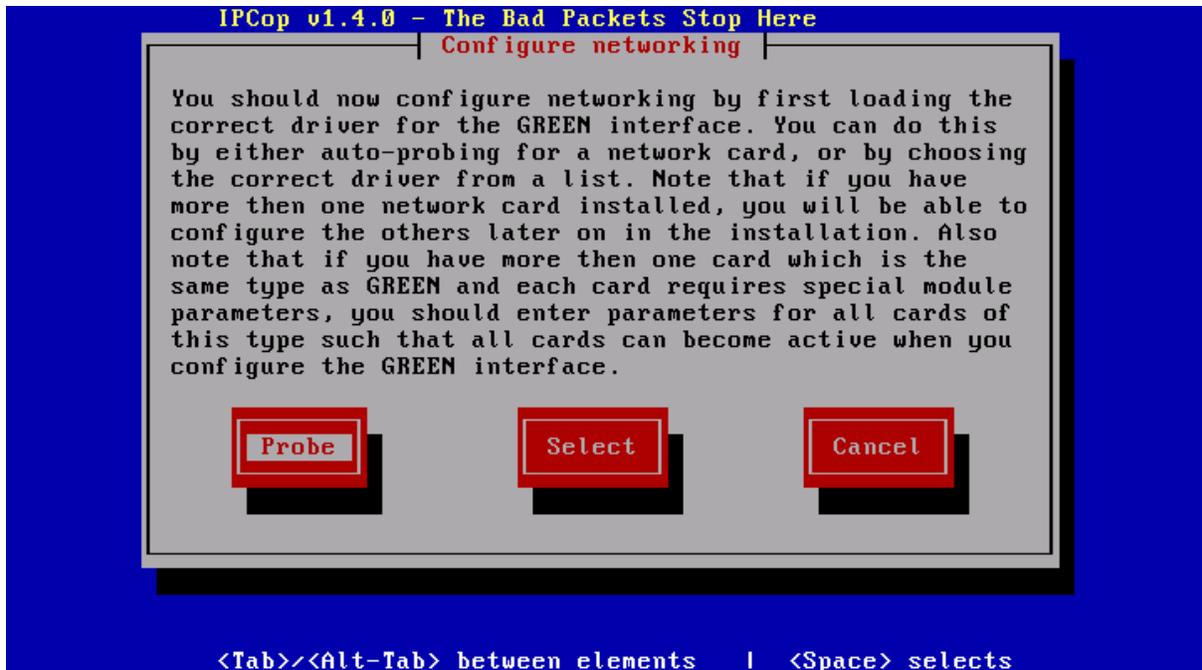
At this point, you have the option of restoring files from an IPCop backup floppy.

To do the restore, place the backup floppy in the floppy disk drive and select Restore and press the **Enter** key. Otherwise, select Skip and press the **Enter** key.

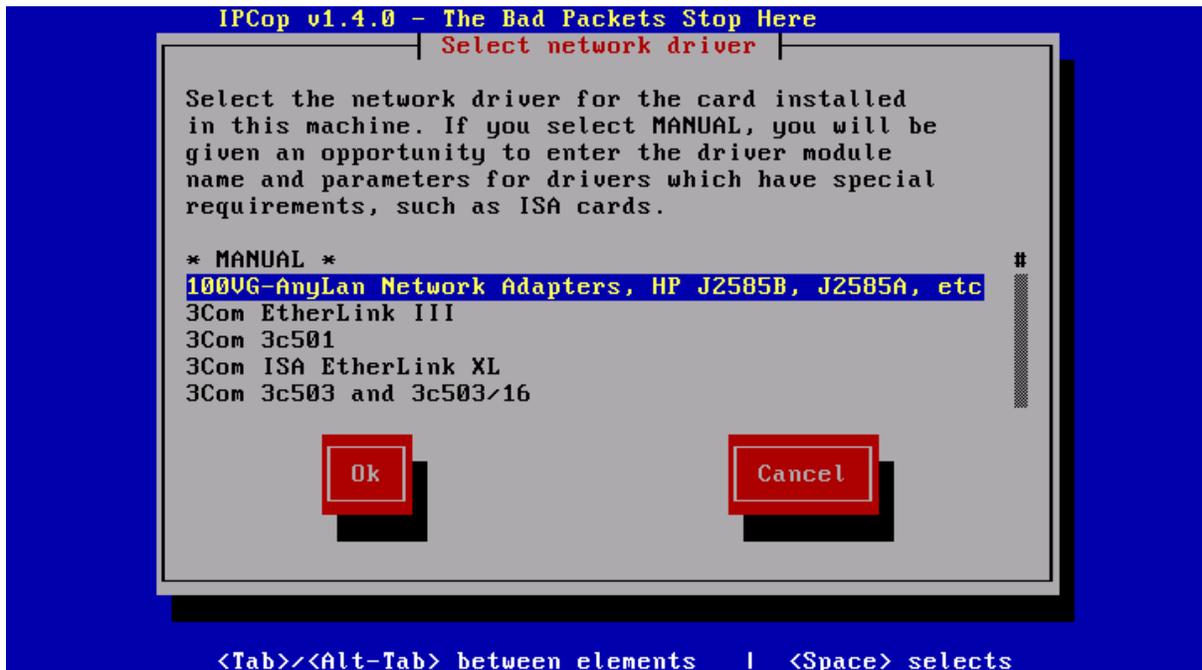
If you are upgrading from a 1.2.0 or later version of IPCop, insert an IPCop backup floppy in your floppy disk drive. This facility is also intended to recover damaged IPCop installations. In fact, after setting up IPCop to your satisfaction, using the web interface, take a backup. If there is a failure, reinstall IPCop using the procedure you used to do the initial installation, and during the install, insert the backup floppy disk, and respond Restore to this prompt. IPCop configuration will be restored.

If you restore from floppy, you will not have to respond to any more dialogs. After the old configuration is restored, the install process will skip to the “Installation Complete” dialog, below.

Next IPCop will begin setting up your GREEN (local) network interface. You can allow IPCop to probe your network card, and automatically select driver parameters. Select the Probe button and press **Enter** to have IPCop probe your hardware. Select the Select button and press **Enter** to manually select a NIC card or specify parameters information you collected from the manufacturer’s driver floppy or the manufacturer’s web page.

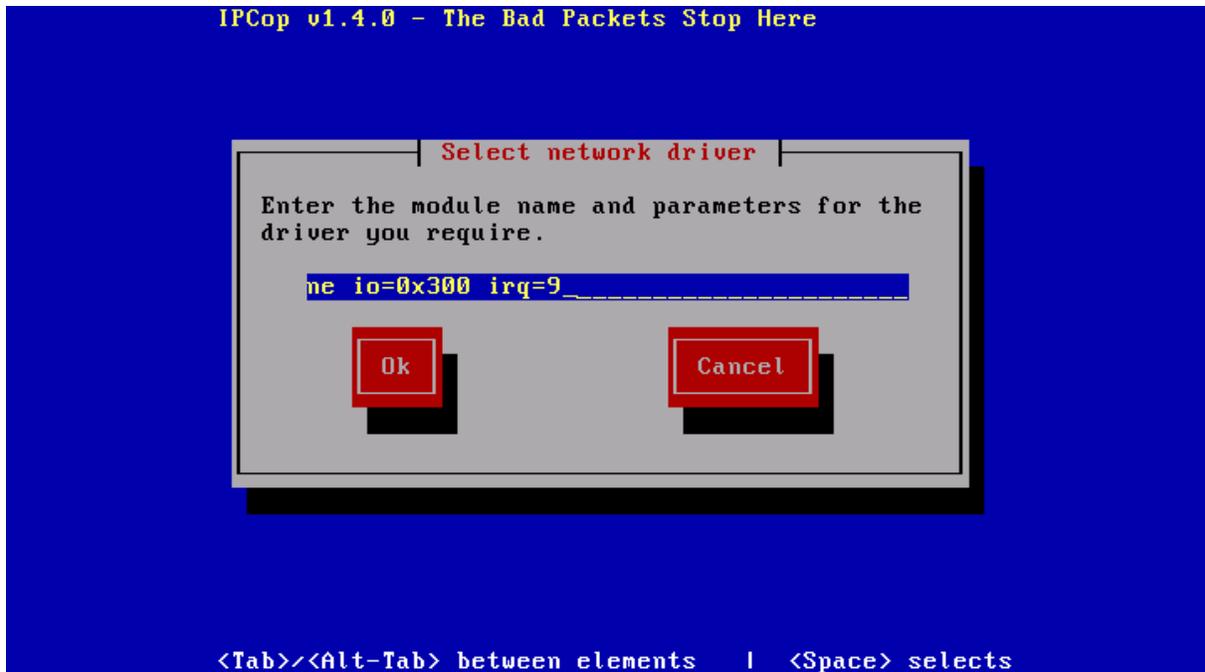


If you specify Select, above, the following screen will appear:

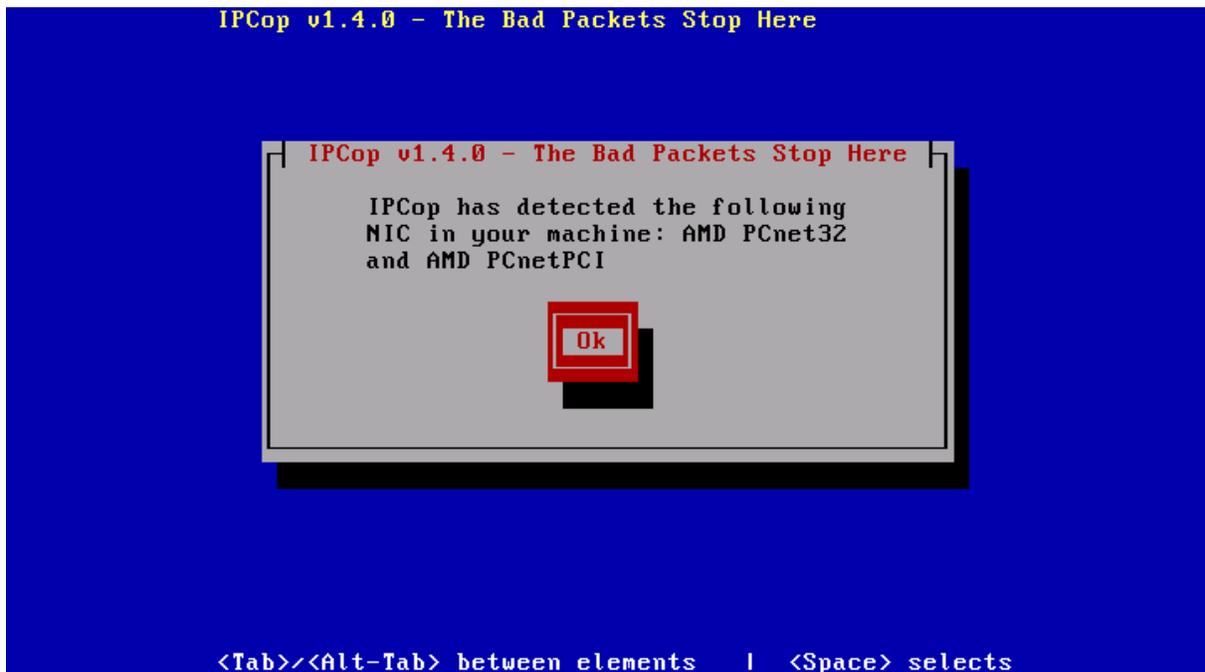


Select your GREEN Ethernet NIC from the list.

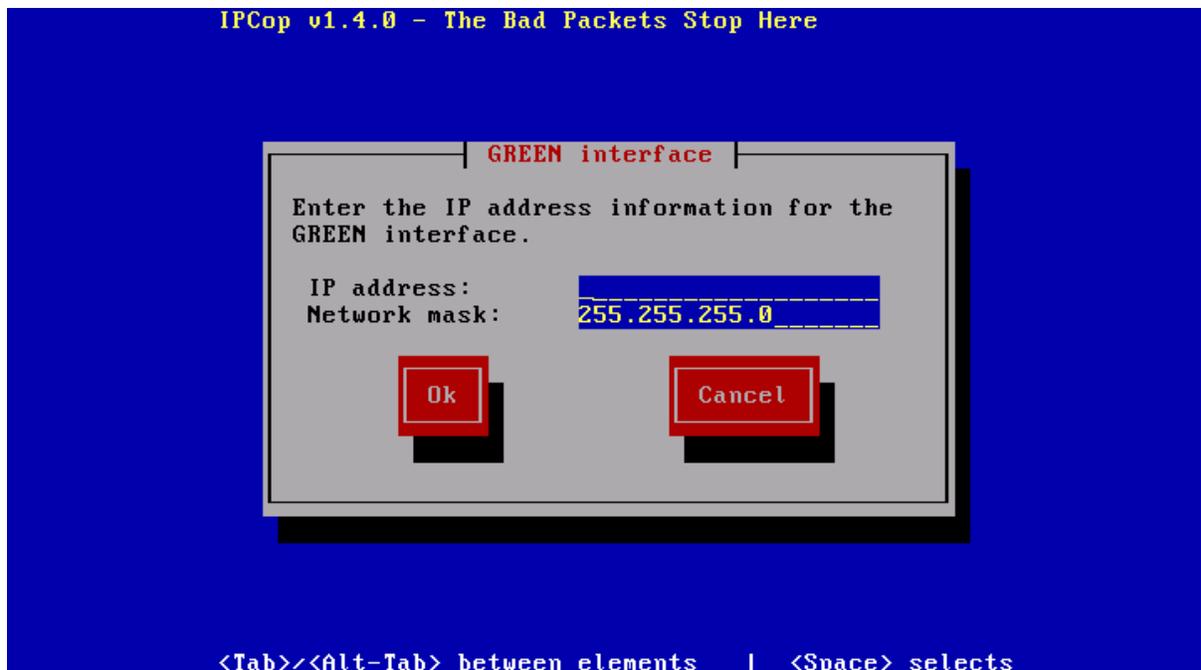
If you select MANUAL the following screen will appear. Enter the object module for the driver you require. Each driver may require extra installation parameters. Unfortunately, these are driver dependent. The sample, below, is for a NE 2000 driver. Like most ISA drivers, it needs both its IO address, *io=*, and IRQ, *irq=*, specified.



If you specify Probe, above, the following screen will appear:



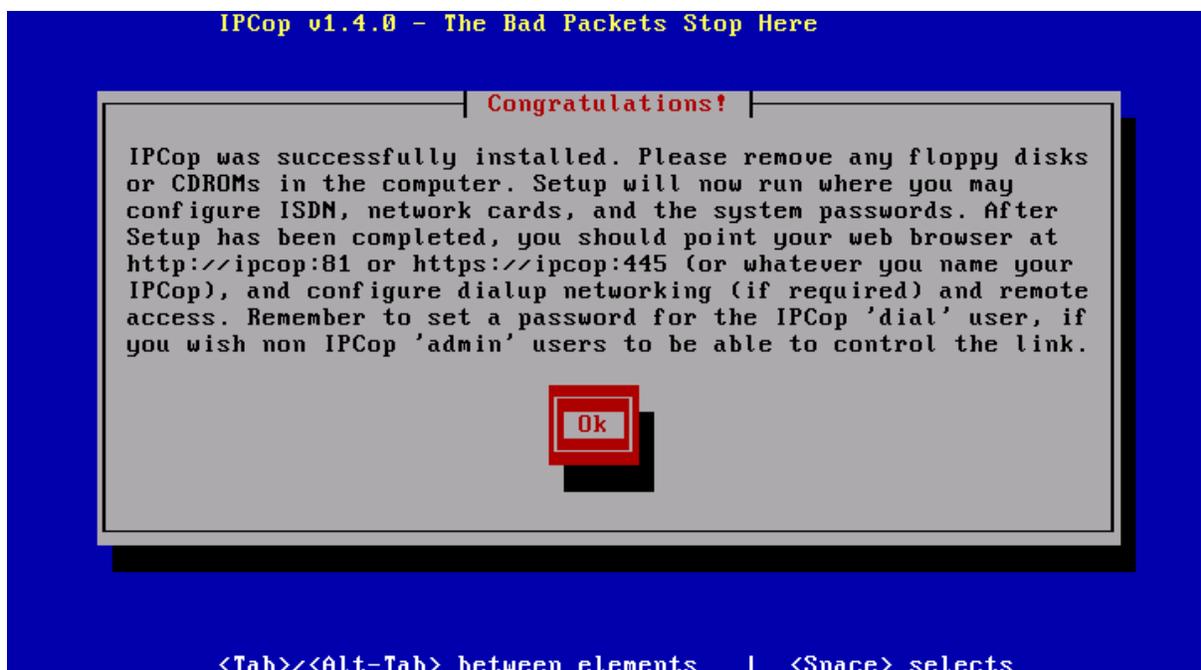
Your NIC card's manufacturer may not appear. IPCop identifies NICs based on the chip manufacturer, not the card manufacturer. This can be ignored.



IPCop will now configure its internal network address, the GREEN interface.

This is an address on the network discussed in [Decide On Your Local Network Address](#), above. Usually, this will be either GREEN address 1, i.e. 192.168.1.1; or GREEN address 254, i.e. 192.168.1.254. Although any address on your GREEN network will do. IPCop will automatically set your Network mask based on your IP address, but you can modify it if you need to.

All of IPCop has now been installed on your hard drive. The following screen will appear. Remove the IPCop CD from your CD drive and, if present, the bootable floppy from the floppy drive. Select Ok to continue.



IPCop will continue with the setup command automatically.

From this point on the Installation process is identical no matter which media was used for the initial boot. Please continue with the Initial Configuration Section, below.

2.2. Installing From Floppy and Web Server or FTP

Put the IPCop CD in the IPCop PC's CD-ROM drive. If necessary, put the IPCop bootable floppy in the floppy drive. Press the reset button to start the boot sequence. If the IPCop PC does not boot, check the BIOS boot parameters.

Soon the boot up screen, below, will appear. If it does not appear, check that your monitor is connected to the video port on the target machine, is powered on and that you have booted from the CD or floppy drive.

```
ISOLINUX 2.08 2003-12-12 Copyright (C) 1994-2003 H. Peter Anvin

Welcome to IPCop, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

-----
----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
----
-----

Press RETURN to boot IPCop default installation.

Or, if you are having trouble you can try these options...

Type:  nopcmcia to disable PCMCIA detection
       nousb to disable USB detection
       nousborpcmcia to disable both PCMCIA & USB detection

boot: _
```

This screen contains a warning that all your existing data will be destroyed.

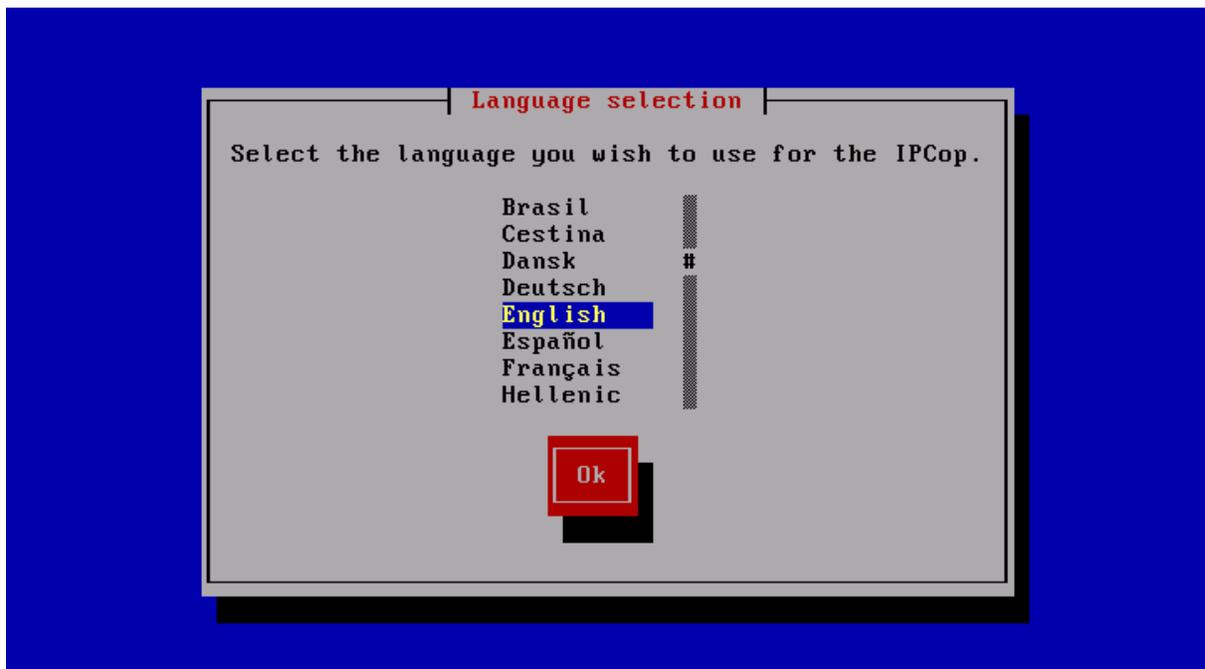
At this point you may just press the **Enter** key, or enter one of the three installation options “nopcmcia”, “nousb” or “nousborpcmcia”. The installation options will restrict the devices that the IPCop installation process detects. Use these options only if the standard installation runs into trouble identifying PCMCIA or USB devices attached to the target machine. You may also eject the IPCop media and reboot to abort the installation.

```
zone(0): 4096 pages.  
zone(1): 61440 pages.  
zone(2): 0 pages.  
Kernel command line: BOOT_IMAGE=vmlinuz ide=nodma initrd=instroot.gz root=/dev/r  
am0 rw  
ide_setup: ide=nodma : Prevented DMA  
Initializing CPU#0  
Detected 1615.700 MHz processor.  
Console: colour UGA+ 80x25  
Calibrating delay loop... 3217.81 BogoMIPS  
Memory: 253900k/262144k available (1142k kernel code, 7792k reserved, 350k data,  
84k init, 0k highmem)  
Dentry cache hash table entries: 32768 (order: 6, 262144 bytes)  
Inode cache hash table entries: 16384 (order: 5, 131072 bytes)  
Mount cache hash table entries: 512 (order: 0, 4096 bytes)  
Buffer cache hash table entries: 16384 (order: 4, 65536 bytes)  
Page-cache hash table entries: 65536 (order: 6, 262144 bytes)  
CPU: Trace cache: 12K uops, L1 D cache: 8K  
CPU: L2 cache: 512K  
Intel machine check architecture supported.  
Intel machine check reporting enabled on CPU#0.  
CPU: Intel(R) Pentium(R) 4 CPU 1.60GHz stepping 08  
Enabling fast FPU save and restore... done.  
Enabling unmasked SIMD FPU exception support... done.  
Checking 'hlt' instruction... _
```

During boot up many kernel informational messages will scroll by.

These can be ignored unless a hardware problem is detected. If an error is detected, the boot may stop.

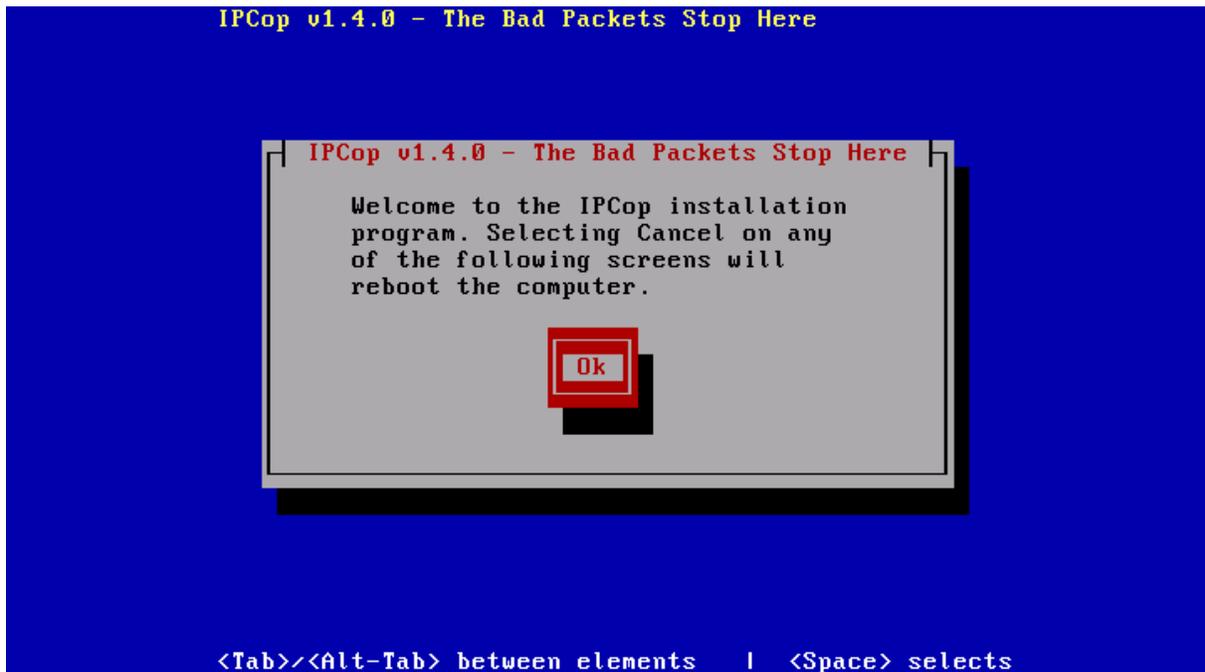
After a few seconds, the language selection screen will appear.



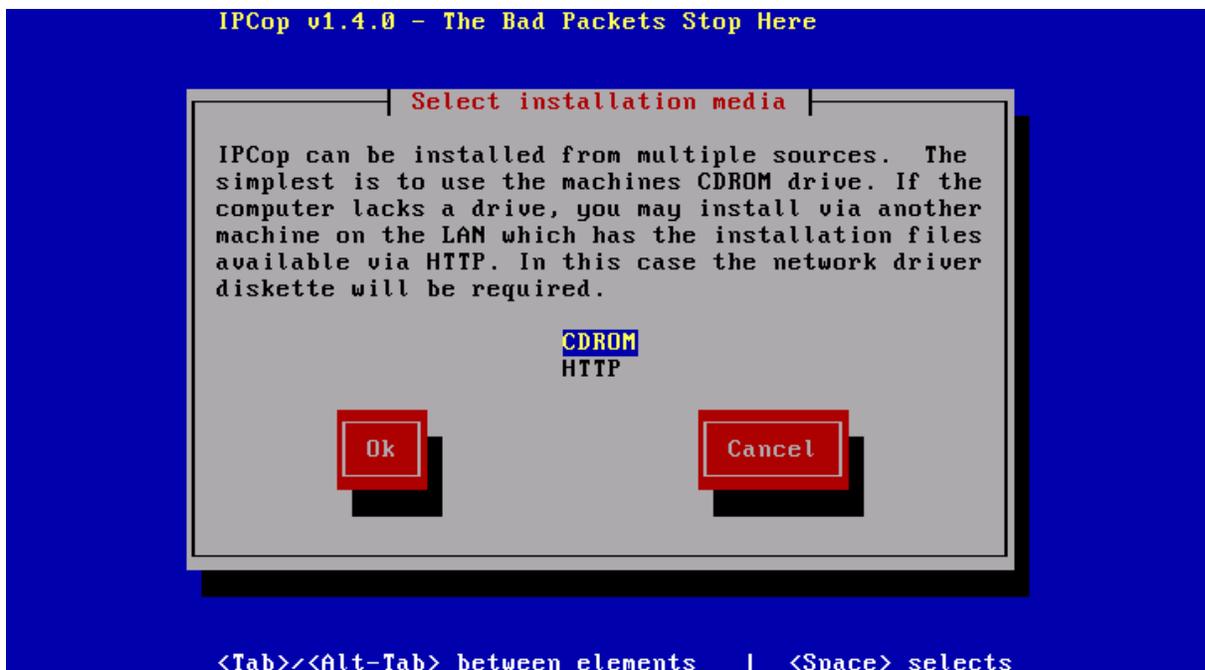
At this time Brazilian Portuguese, Czech, Danish, German, Greek, English, Spanish, French, Hungarian, Italian, Latin American Spanish (Latino), Dutch, Norwegian, Portuguese, Finnish, Swedish, and Turkish are available.

Note: On this and all other installation screens, the mouse is ignored. To move the cursor around the screen, use the **Tab** key and the keyboard arrow keys. To select an item, press the **Space** key. To accept the language choice, press the **Enter** key.

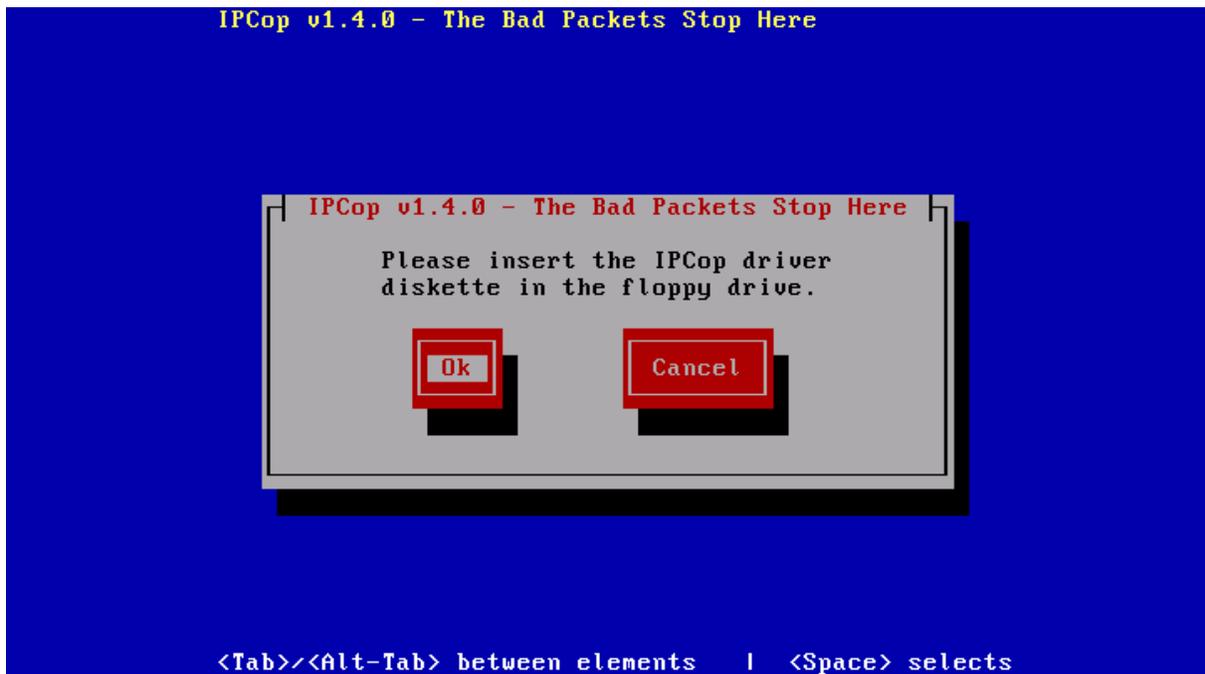
From this point on, in the install, all dialogs, menus and web pages will appear in your chosen language.



The next screen simply informs you of how to abort the installation. " Select the Cancel and press the **Enter** key. "



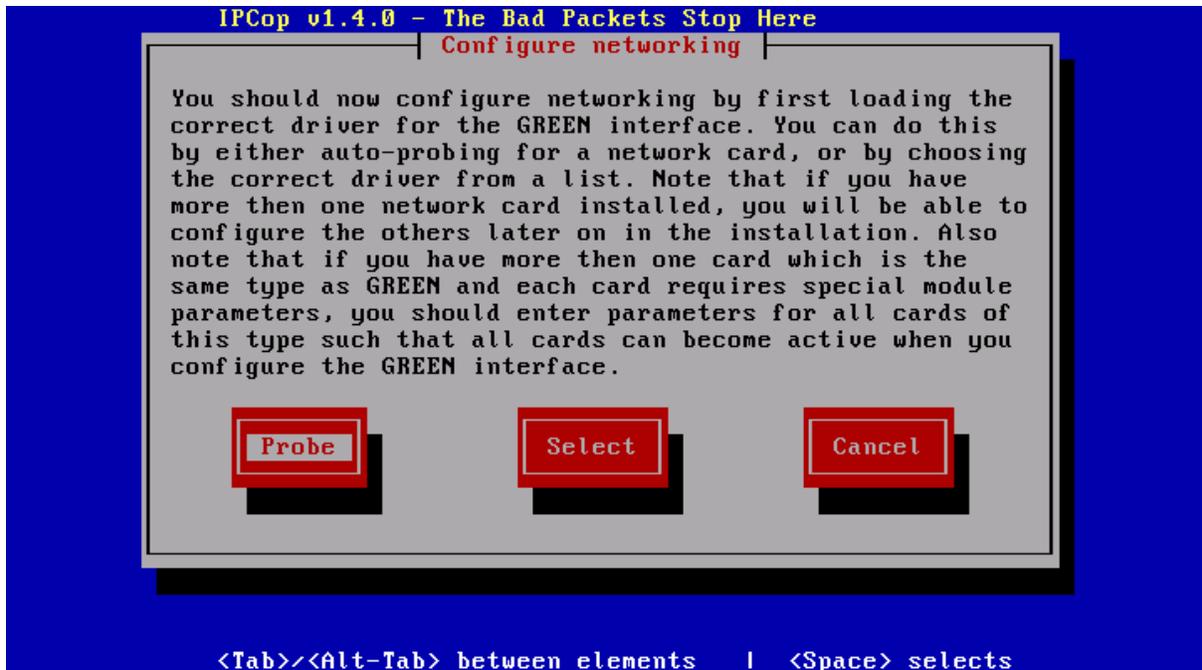
The next dialog box lets you choose the installation media. Since you are installing from HTTP, select it, tab to the Ok button and press the **Enter** key.



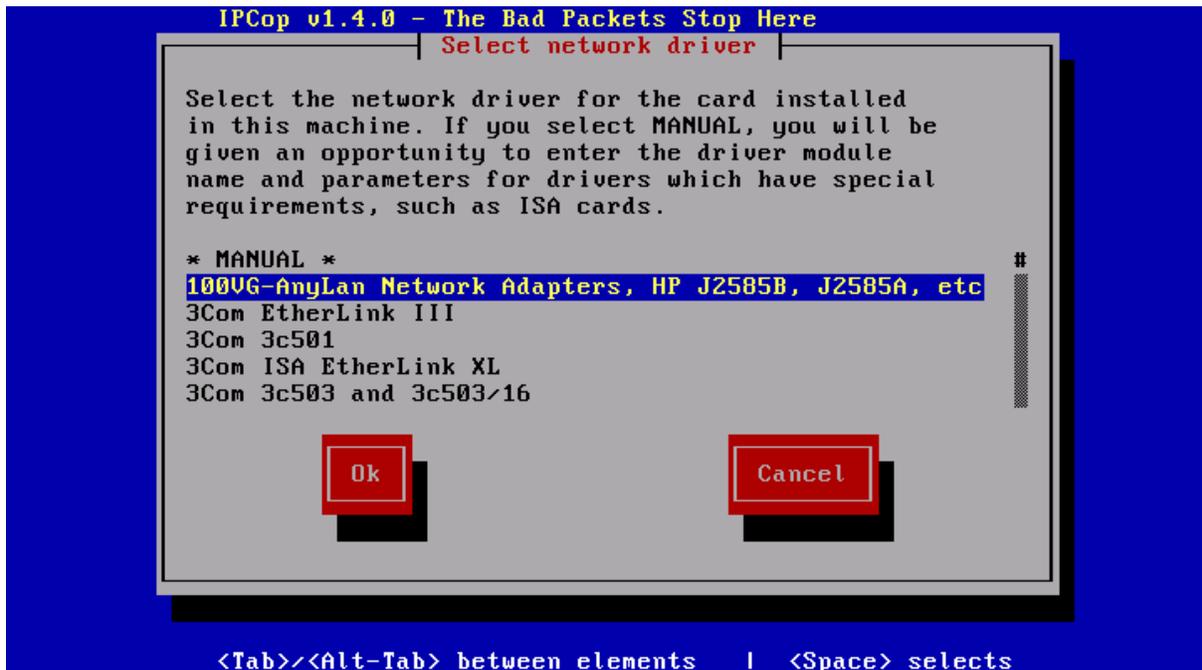
IPCop will ask you to replace the boot floppy with the driver floppy, created above.

Please do so. Then select the Ok.

Next IPCop will begin setting up your GREEN (local) network interface. You can allow IPCop to probe your network card, and automatically select driver parameters. Select the Probe button and press **Enter** to have IPCop probe your hardware. Select the Select button and press **Enter** to manually select a NIC card or specify parameters information you collected from the manufacturer's driver floppy or the manufacturer's web page.

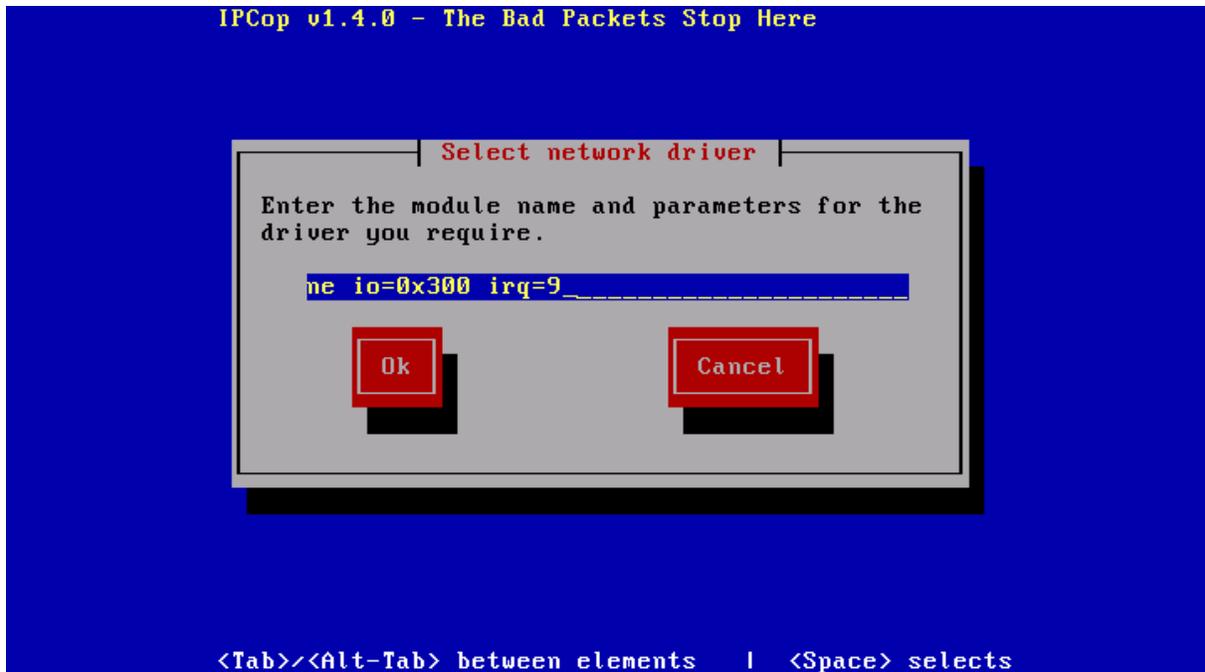


If you specify Select, above, the following screen will appear:

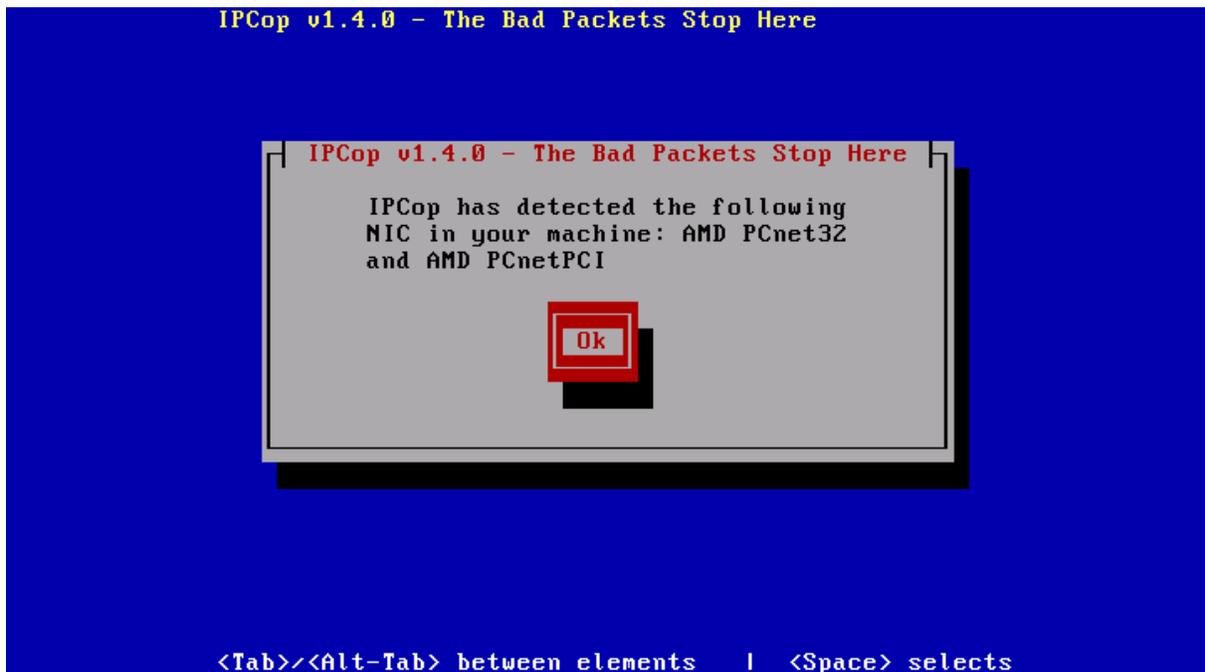


Select your GREEN Ethernet NIC from the list.

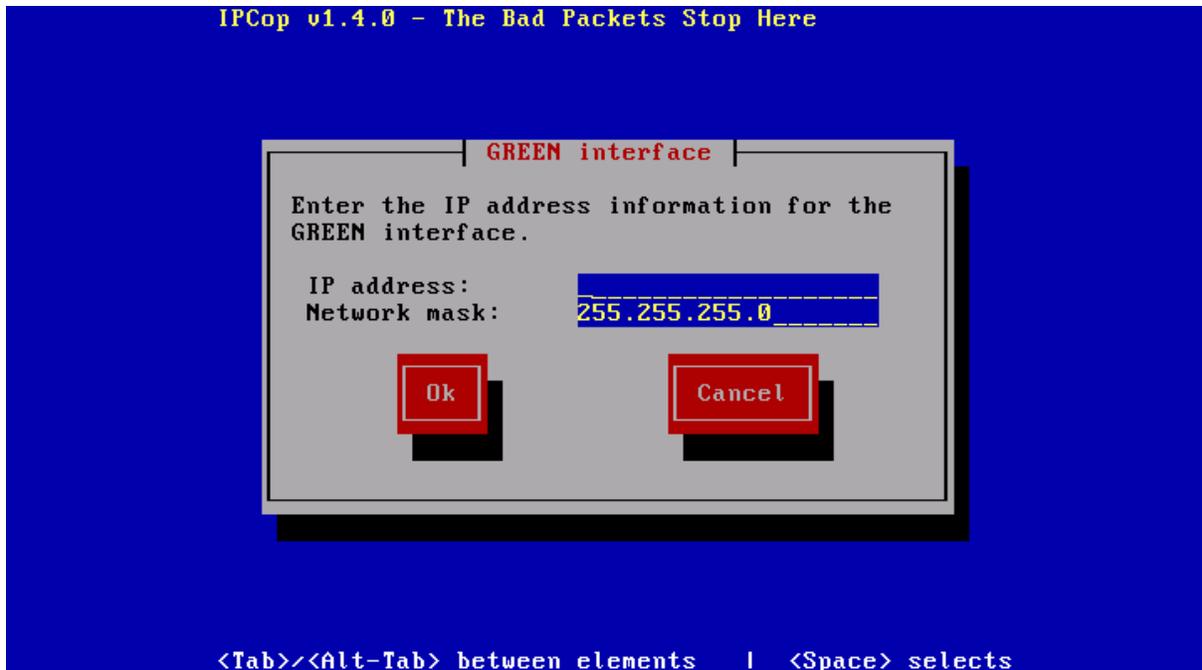
If you select MANUAL the following screen will appear. Enter the object module for the driver you require. Each driver may require extra installation parameters. Unfortunately, these are driver dependent. The sample, below, is for a NE 2000 driver. Like most ISA drivers, it needs both its IO address, *io=*, and IRQ, *irq=*, specified.



If you specify Probe, above, the following screen will appear:



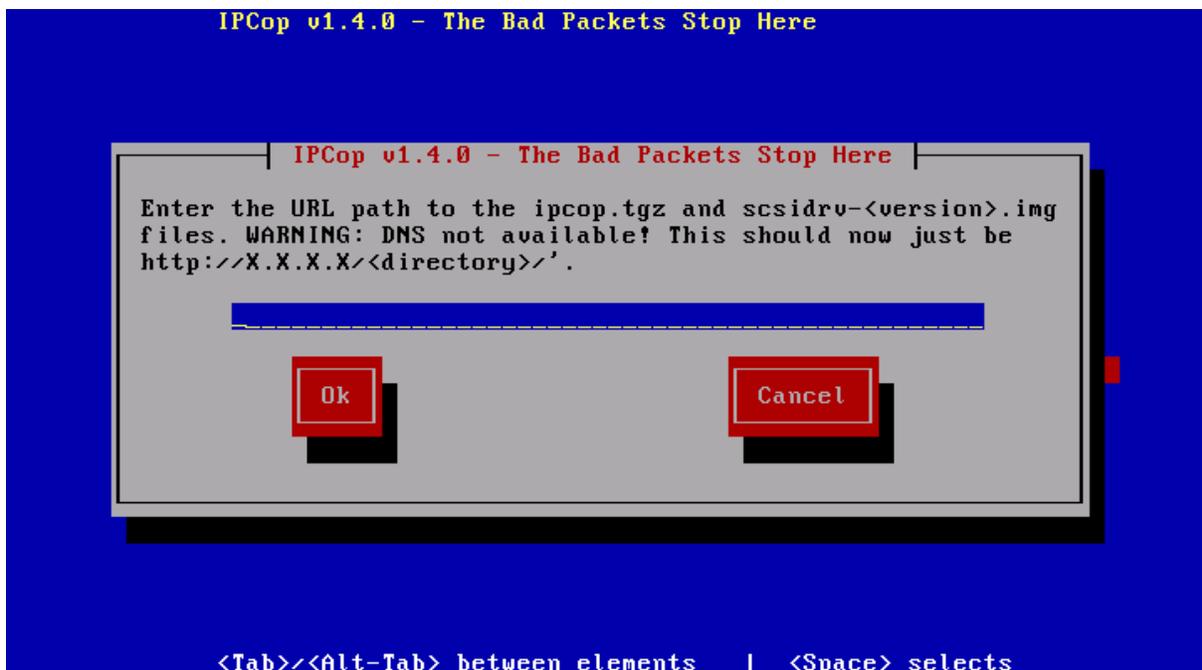
Your NIC card's manufacturer may not appear. IPCop identifies NICs based on the chip manufacturer, not the card manufacturer. This can be ignored.



IPCop will now configure its internal network address, the GREEN interface.

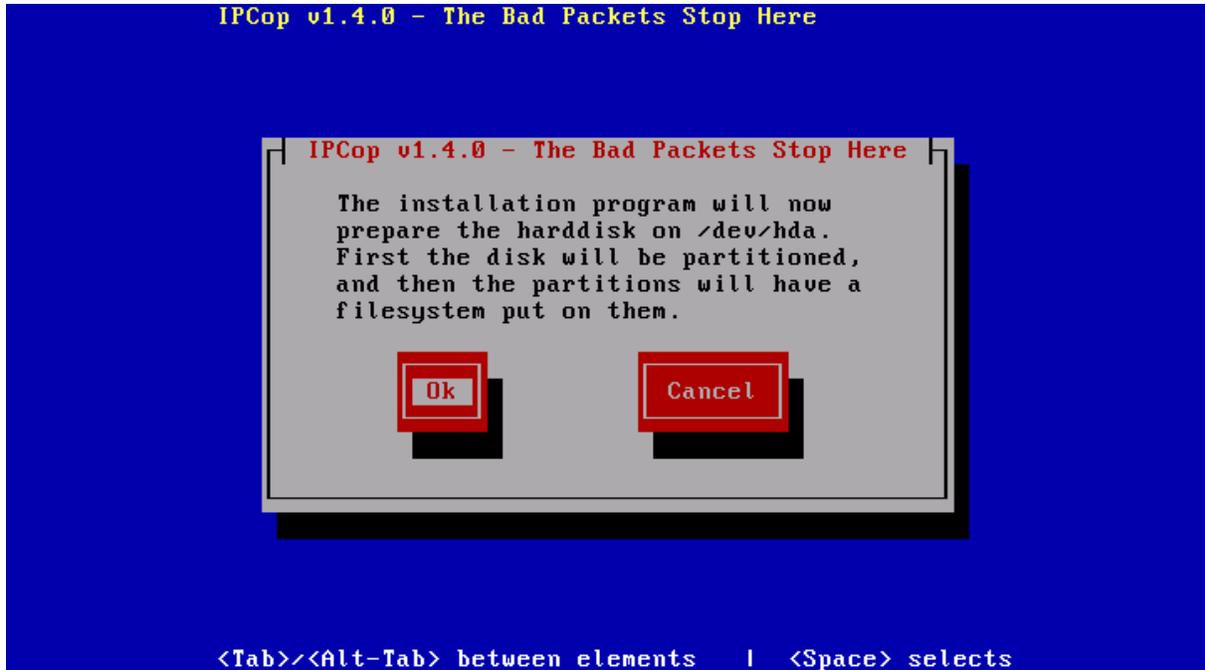
This is an address on the network discussed in [Decide On Your Local Network Address](#), above. Usually, this will be either GREEN address 1, i.e. 192.168.1.1; or GREEN address 254, i.e. 192.168.1.254. Although any address on your GREEN network will do. IPCop will automatically set your Network mask based on your IP address, but you can modify it if you need to.

This network will be used to locate and download the IPCop installation file from your web or FTP server.



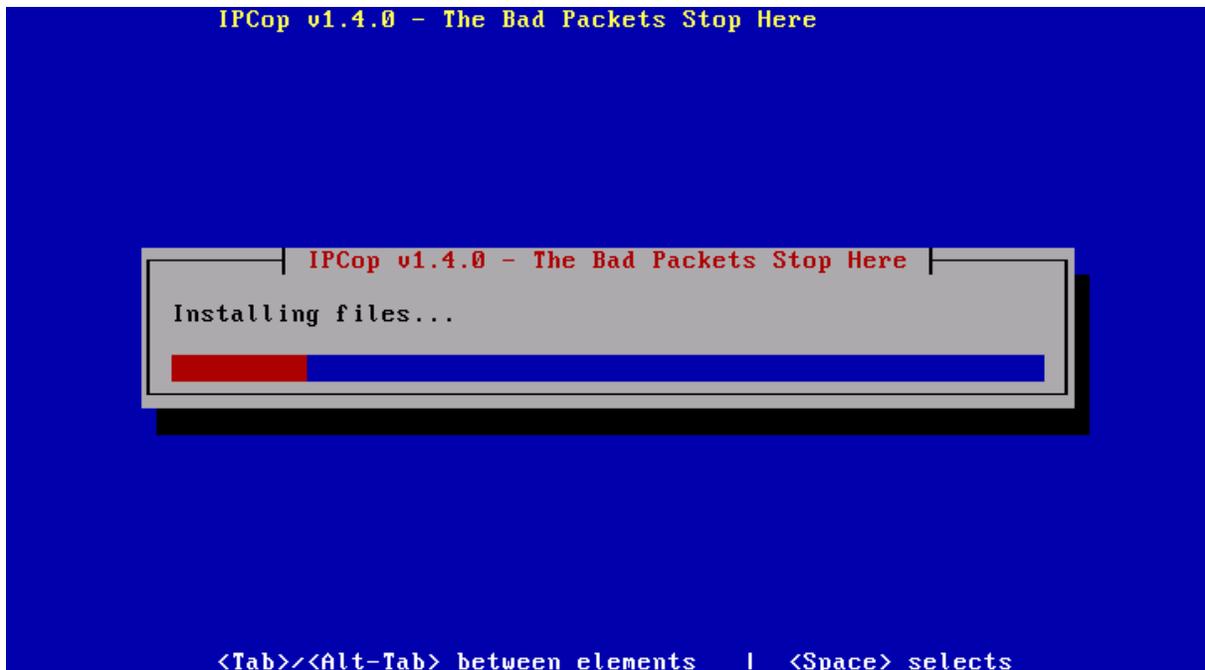
The IPCop installation will now ask for the URL of the directory containing the `ipcop-1.4.0.tgz` and `scsidrv-1.4.0.img` files you placed on your web or FTP server earlier.

Enter `ftp` or `http` depending on the server, and use the IP address of your server. For example: `ftp://192.168.1.2/pub/`. Don't forget to specify the directory not the file and to end with a `/`.

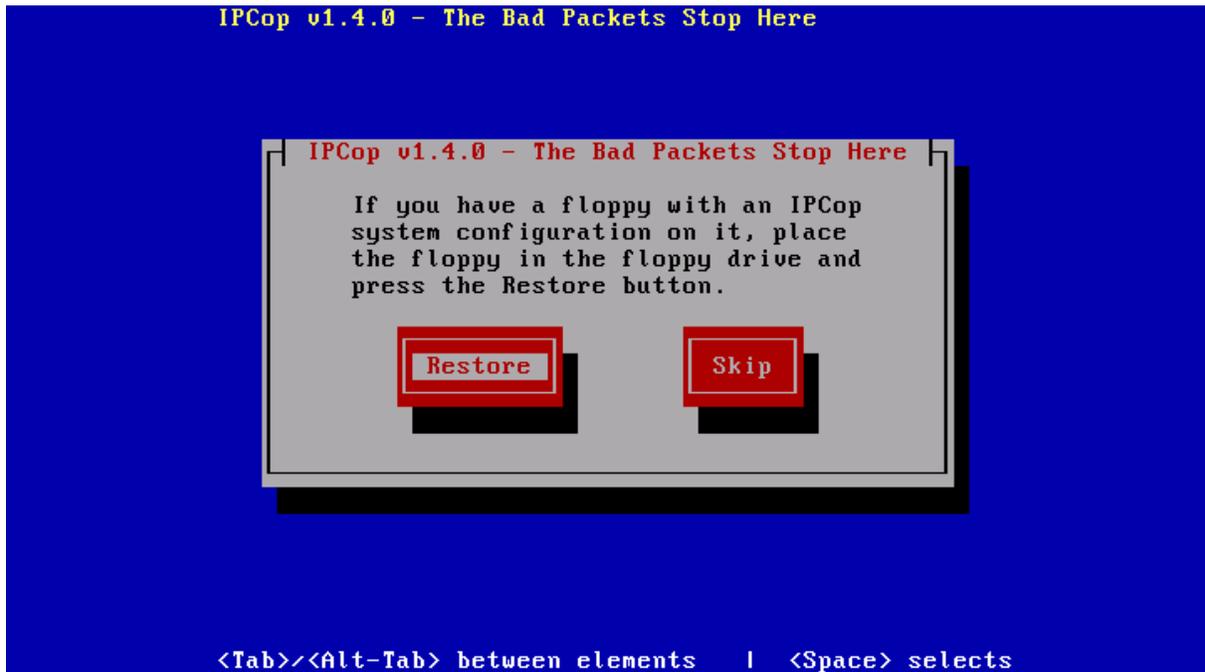


Your final warning appears next.

After you select **Ok** and press **Enter** on this screen all of the data on your hard drive will be erased. To abort the installation, select **Cancel** and press the **Enter** key.



Next IPCop will format and partition your hard drive. Then it will install all its files.

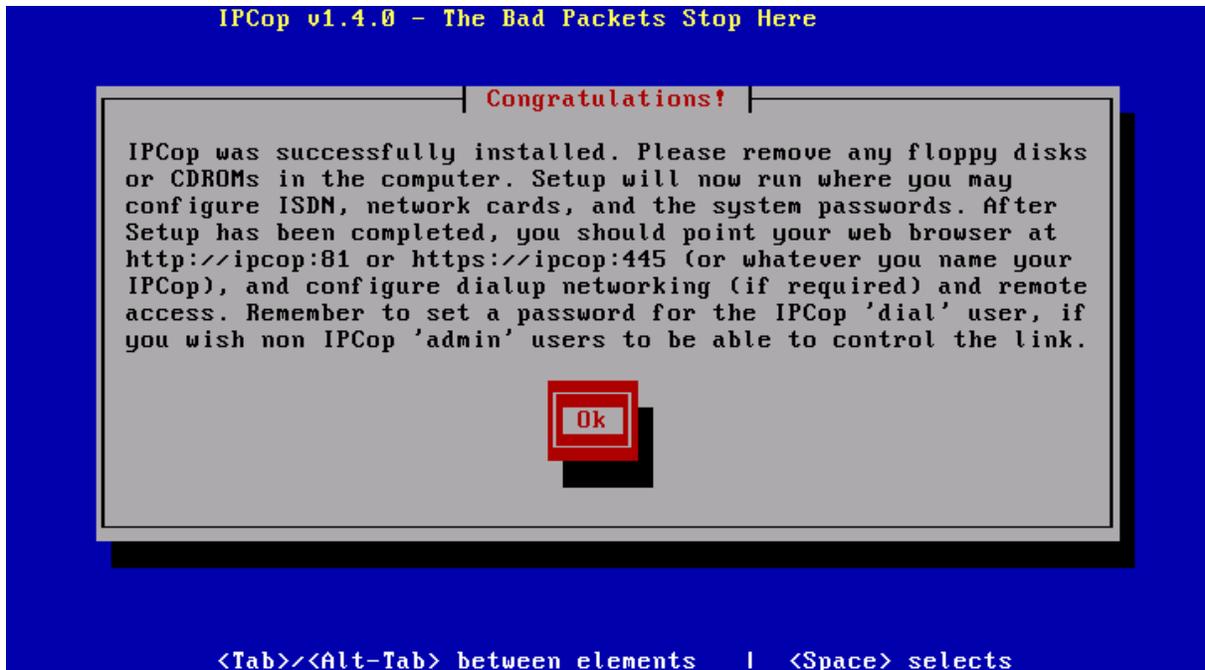


At this point, you have the option of restoring files from an IPCop backup floppy.

To do the restore, place the backup floppy in the floppy disk drive and select Restore and press the **Enter** key. Otherwise, select Skip and press the **Enter** key.

If you are upgrading from a 1.2.0 or later version of IPCop, insert an IPCop backup floppy in your floppy disk drive. This facility is also intended to recover damaged IPCop installations. In fact, after setting up IPCop to your satisfaction, using the web interface, take a backup. If there is a failure, reinstall IPCop using the procedure you used to do the initial installation, and during the install, insert the backup floppy disk, and respond Restore to this prompt. IPCop configuration will be restored.

If you restore from floppy, you will not have to respond to any more dialogs. After the old configuration is restored, the install process will skip to the “Installation Complete” dialog, below.



IPCop will continue with the setup command automatically.

From this point on the Installation process is identical no matter which media was used for the initial boot. Please continue with the Initial Configuration Section, below.

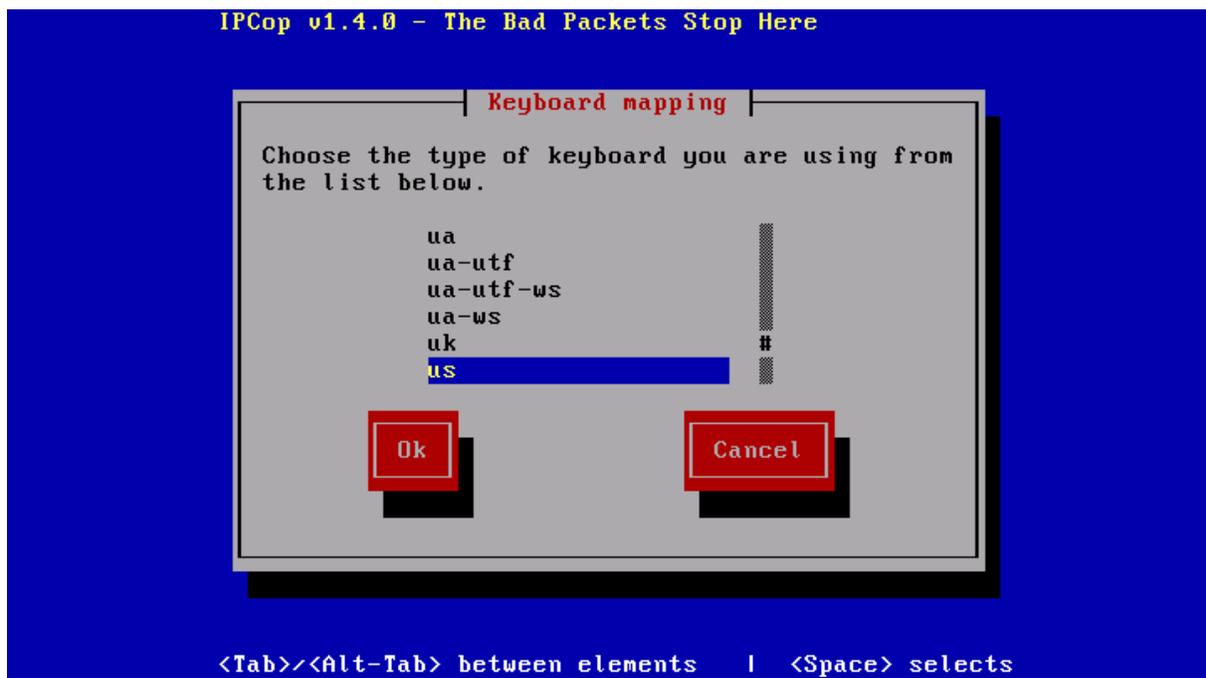
Chapter 3. Initial Configuration

For all install media IPCop will automatically continue with its installation, by setting up its initial configuration.

Warning

If you cancel out of the initial configuration before setting the root password you will not be able to log in as root to complete setup. In this case, you can reboot your machine and enter what is called “single user” mode to add your root password. Please see Loss of the Root Password.

After reboot, log in as root and enter the setup command. You will be able to verify and setup all remaining IPCop parameters by going to each menu item and filling the parameters.



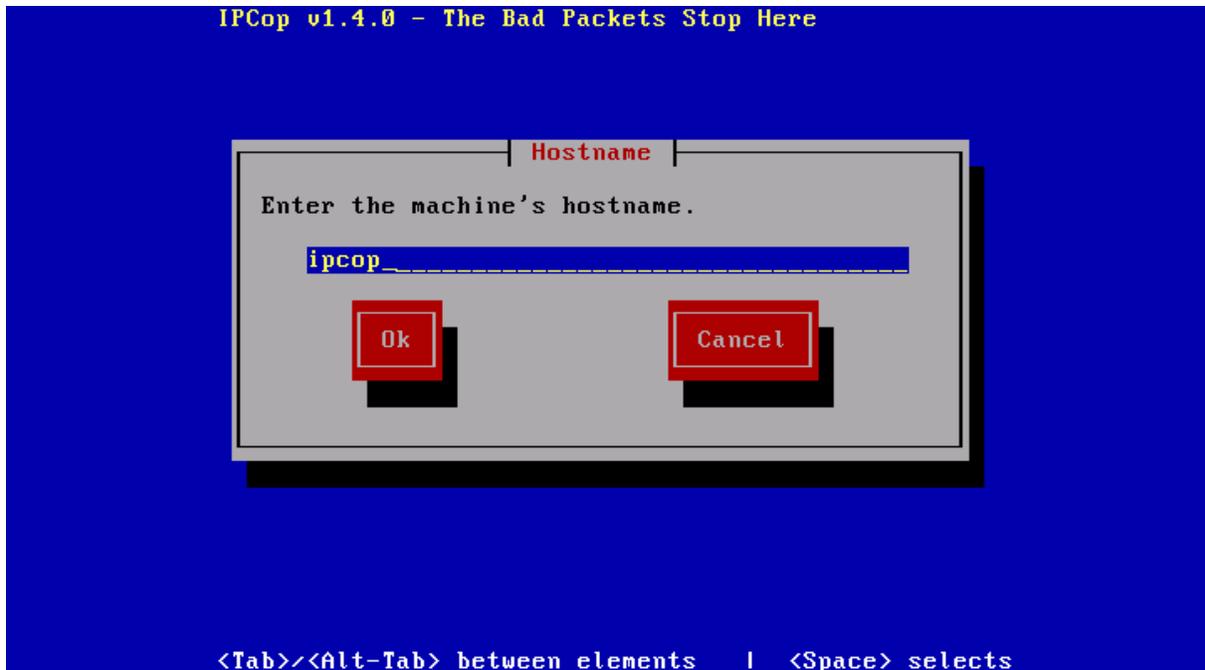
The first screen allows you to configure your keyboard.



The next screen, above, asks for your time zone.

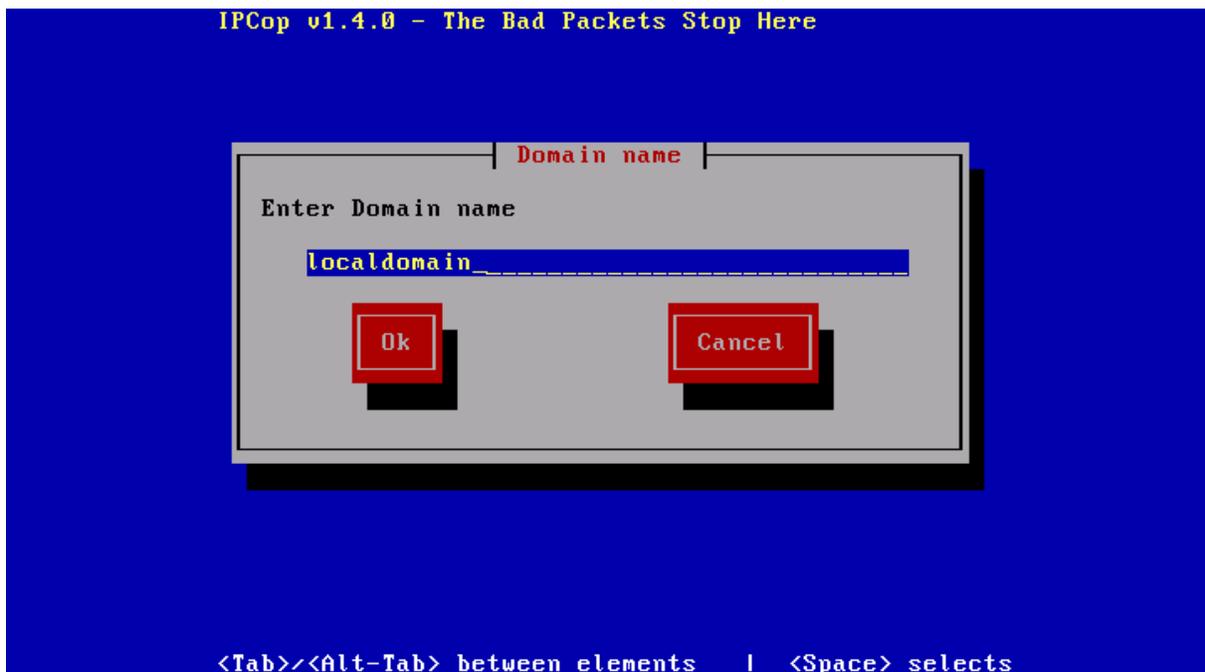
Some people leave the time zone as London or UTC. This allows you to leave your PC's hardware clock set to the local time. There are a couple of disadvantages to this setting:

- You will not be able to use a network time server to accurately set your PC's time, via the Time Administrative Web Page [<http://www.ipcop.org/1.4.0/en/admin/html/system.html#time>].
- If your local time zone changes from Winter to Summer or Daylight Savings to Standard time, you will have to remember to manually change the IPCop PC's clock. If you set the time zone to your correct time zone, IPCop will automatically change the time for you.



You must then configure your IPCop machine's hostname.

The default of "ipcop" is fine. You may want to change this if you are planning on setting up a VPN and allowing administration across your VPN. In this case you may want to give each IPCop machine a unique hostname, such as "ipcop1", "ipcop2", "millie", "steve", "bob", etc.



You must then configure your IPCop machine's domain name.

If you have a domain name then enter it here. If you do not have one or do not wish to use it then just accept the default "localdomain". If you plan on using a VPN, you may wish to add additional qualifiers in front of "localdomain" such as "x.localdomain" and "y.localdomain".

It may also be a bad idea to use your real domain name for this purpose, unless you will use your official name server instead of IPCop's domain name server.

This domain name will be automatically set as IPCop's DHCP server's "domain name suffix". Please see the DHCP server discussion.

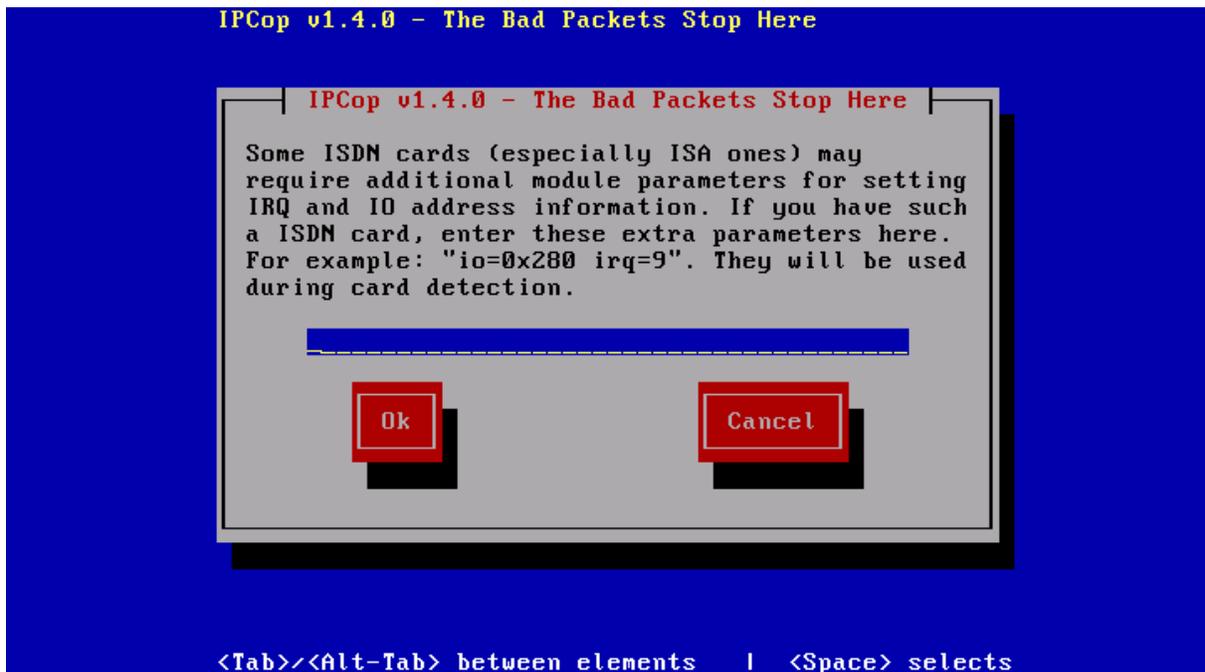


IPCop will continue with the setup command automatically.

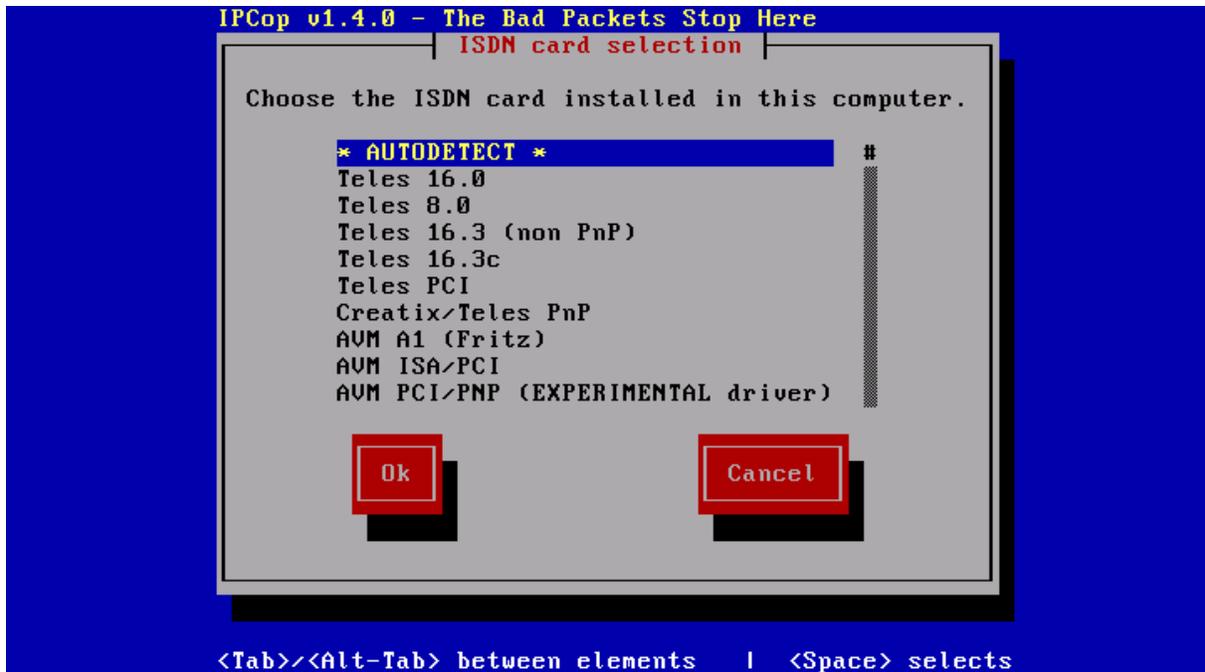
The next screen starts a series of dialogs that will help you set up your ISDN card. If you do not have an ISDN card, select Disable ISDN, and setup will continue with network setup.



If you do have an ISDN modem, select the protocol and country.

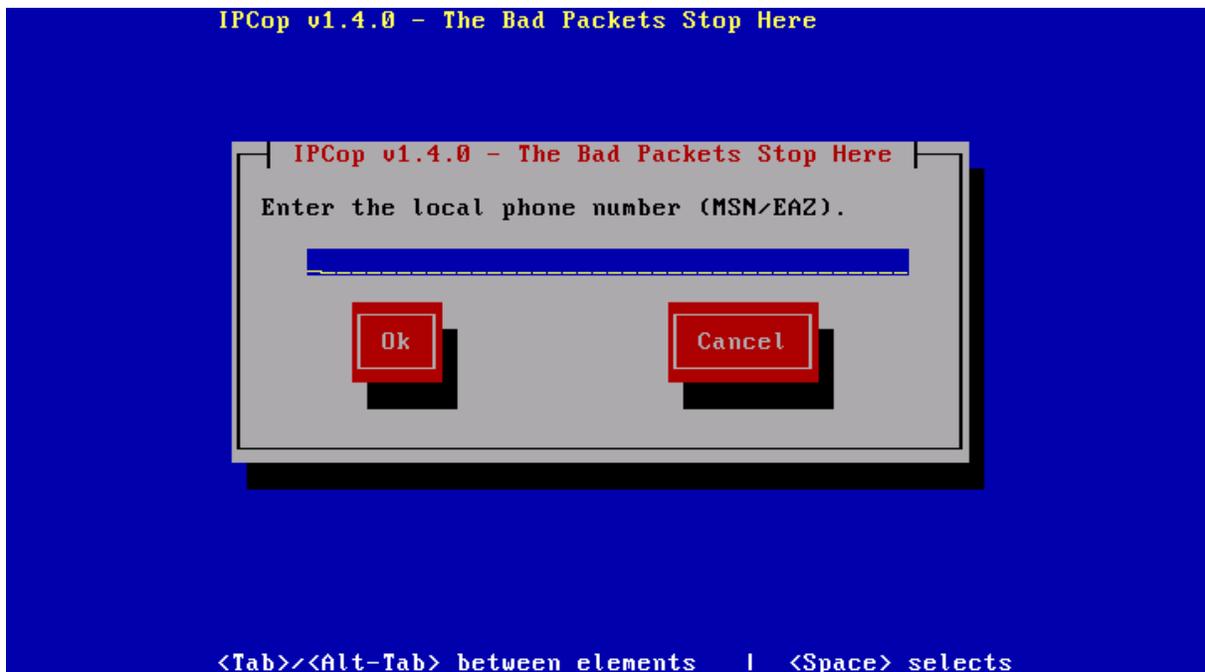


After setting protocol and country, you may need to set driver parameters for your card, especially if it's an ISA card. If so, select Set additional module parameters.

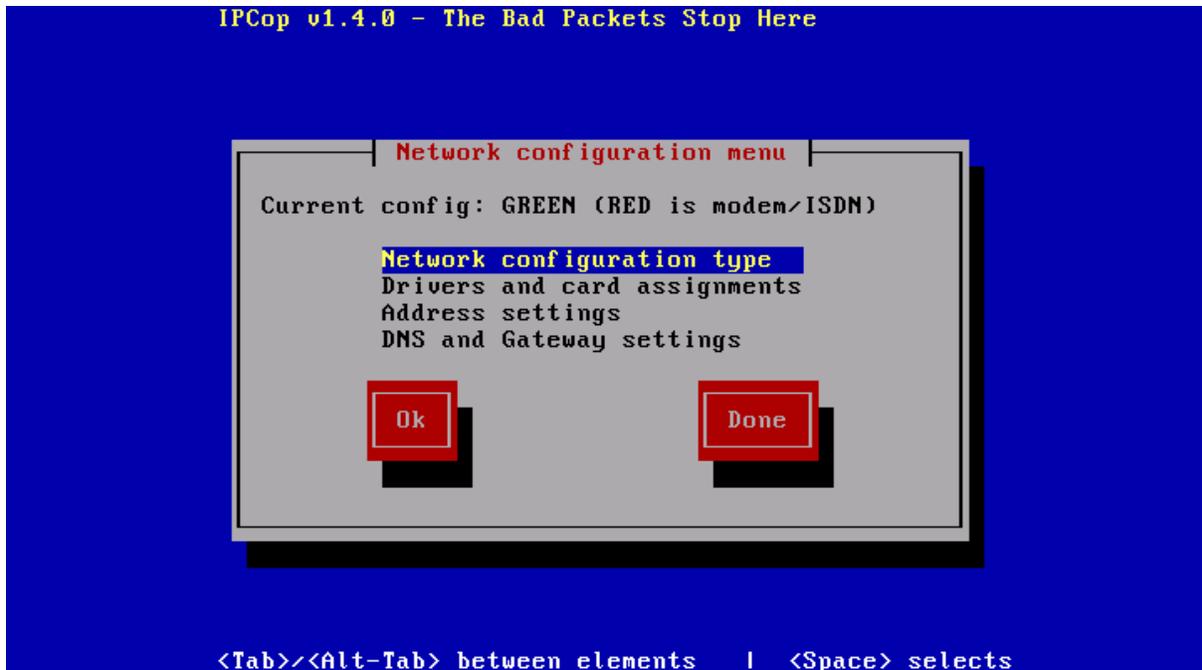


Next you must select the type of ISDN card you have.

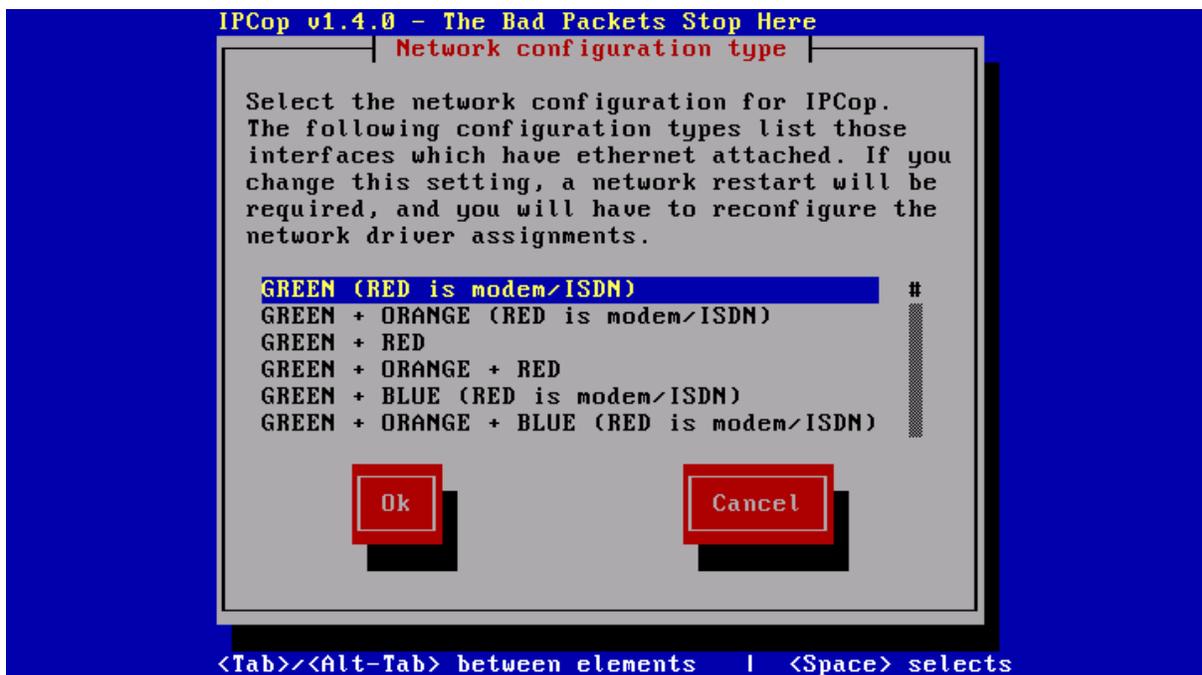
IPCop will probe for the card type, if you select AUTODETECT. If necessary, you can manually select the card you have.



The final step in setting up your ISDN card is setting its local phone number.



Next you will configure your network interfaces. The Network Configuration Menu will take you through the steps necessary to configure them.



As mentioned, above, there are four network interfaces supported by IPCop, RED, GREEN, BLUE and ORANGE.

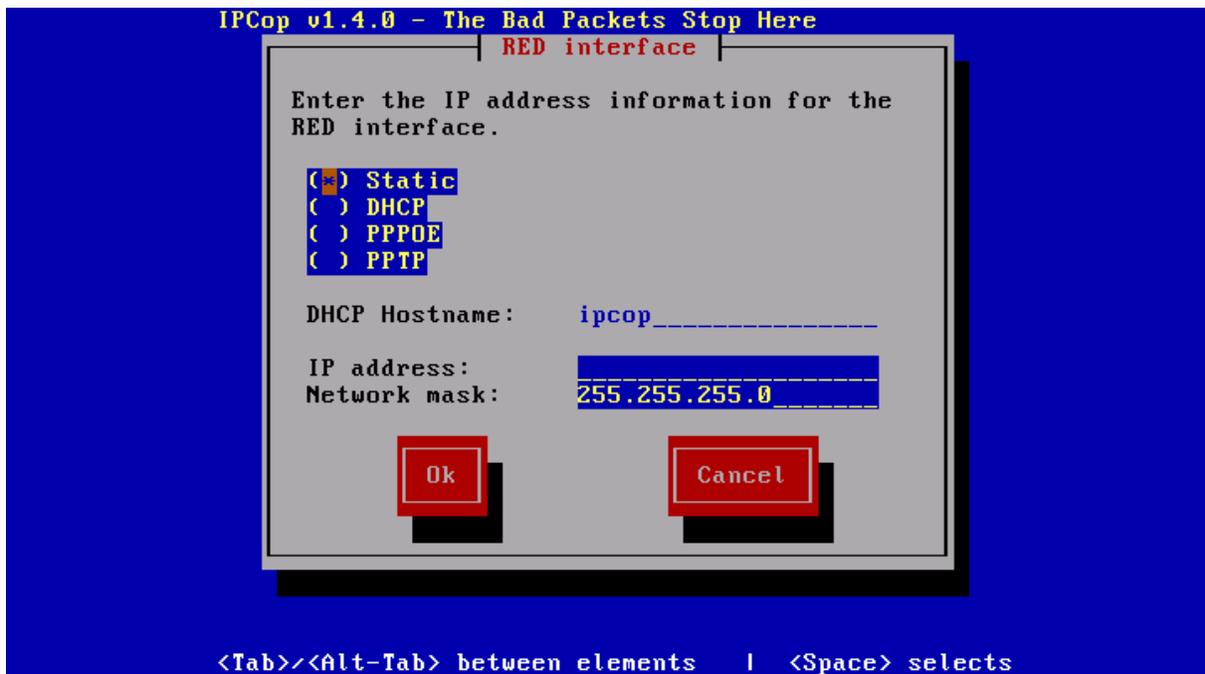
The RED interface is considered the hostile network and can connect via Ethernet, ISDN, analog or ADSL modem. This dialog lets you choose your network configuration type.

When you select Ok, you will be returned to the Network Configuration Menu, above. Tab to the Drivers and card assignments line, select it and press the **Enter** key.

If you have ORANGE and/or BLUE networks, repeat the driver configuration steps you used to configure your GREEN interface. If your RED interface uses an Ethernet connection, configure it, too.

If your RED interface does not use an Ethernet connection, skip to the discussion about configuring additional network interfaces.

After configuring your Ethernet card and driver information for the other interfaces, return to the Network Configuration Menu by selecting the Done button.



Configure the network addresses of the other networks.

Finally, if your RED network is connected via an Ethernet NIC, you will have to configure the way your interface gets its IP address information. This is dependent on your ISP and connection.

Static addressing is used when your ISP has supplied you with a permanent IP address. Enter it in the IP address box of the dialog. IPCop will automatically choose a Network mask. You may modify the network mask as needed.

Your RED network *must* have a static address if you wish to use IPCop's aliasing feature.

DHCP is used when your ISP has indicated you are to use automatic addressing.

Some ISP's, require you to provide a hostname to their DHCP server. This probably is not IPCop's hostname. If it's needed, you can probably use the first part of the fully qualified domain name you noted while gathering the network parameters, above.

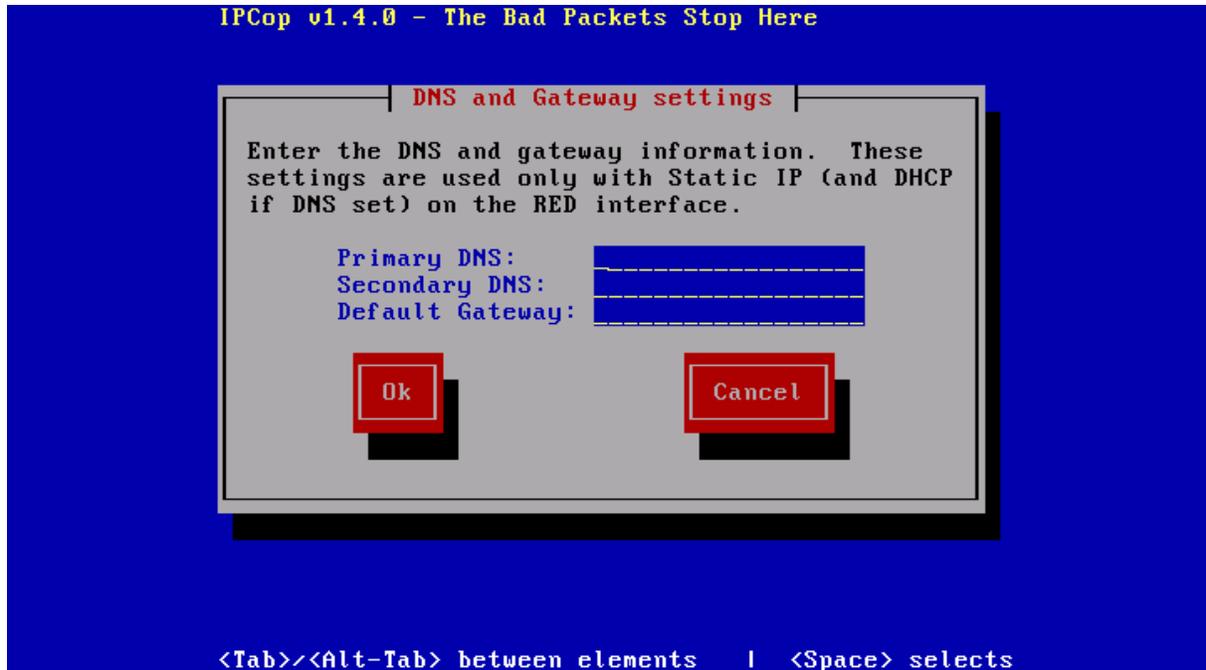
If your connection is via PPPOE, your ISP will supply all necessary information during the initial connection, so you won't have to do anything, after selecting it.

If your connection is via PPTP, you will have to supply your RED network IP address and Network mask, just like the static addressing case. This address is almost always 10.0.0.150 with a network mask of 255.255.255.0.

You may choose to configure an ORANGE or BLUE interface. Their configuration is identical to the way you configured your GREEN interface, above. All three network addresses must be on different networks, i.e. 192.168.1.1, 192.168.2.1, and 192.168.3.1.

You can even reconfigure your GREEN interface at this time, by selecting it from the interface menu.

When you are done, select the Ok button, to return to the Network Configuration Menu.

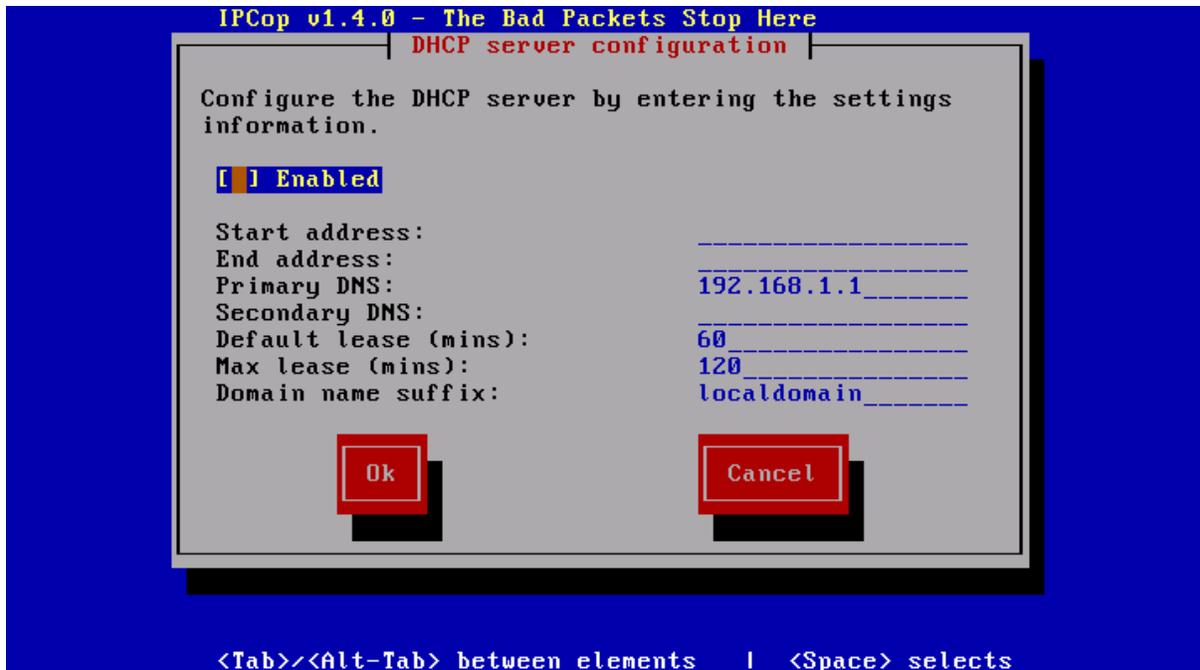


Configuring DNS Servers and Gateways

The next item in the Network Configuration Menu allows you to configure your ISP's DNS servers and your default gateway. You will only need to use this dialog if you are using a static IP address configuration for your RED interface.

Warning

If you configure IPCop with a static IP address, then you add DNS servers or a default gateway using this dialog. If you subsequently change your RED network to use another method for obtaining its address, the servers in this dialog will override those supplied by your ISP. On one hand, this is a good way to override parameters. On the other hand, this can cause endless confusion. When switching from static IP addressing remember to clear these values.



If you are planning to run a DHCP server on IPCop you can configure it at this time. Otherwise, do not enable the server, and continue with setting passwords, below.

Dynamic Host Configuration Protocol allows computers to configure their network interfaces when they are booted.

You can delay setting up IPCop's DHCP server until after the installation completes. See the Administration Manual [http://www.ipcop.org/1.4.0/en/admin/html/services.html#services_dhcp] for a description of the web based method of enabling and configuring the DHCP server.

You must select Enabled to enable the DHCP server.

The Start address and End address define a range of addresses that IPCop's DHCP server will assign to computers when they ask for an address. Do not use your full network range for DHCP. At a minimum leave out IPCop's address. As a practical matter, at some future point in time you may wish to run servers that are only accessible from within your GREEN network. Whether they run FTP servers, web servers, sendmail or any other service that needs a permanent address. These servers should be assigned IP addresses outside the dynamic DHCP range. A good range might be from 192.168.1.200 to 192.168.1.250. This will allow 51 concurrently connected computers on your GREEN network.

DHCP will pass out one or two DNS server addresses in addition to IP addresses. If you wish to run IPCop's DNS proxy, the first should be IPCop's IP address. You can enter a second DNS address as well. If you do not want to use IPCop's DNS proxy and are using Static IP addresses, use the DNS servers you specified while setting up your RED interface.

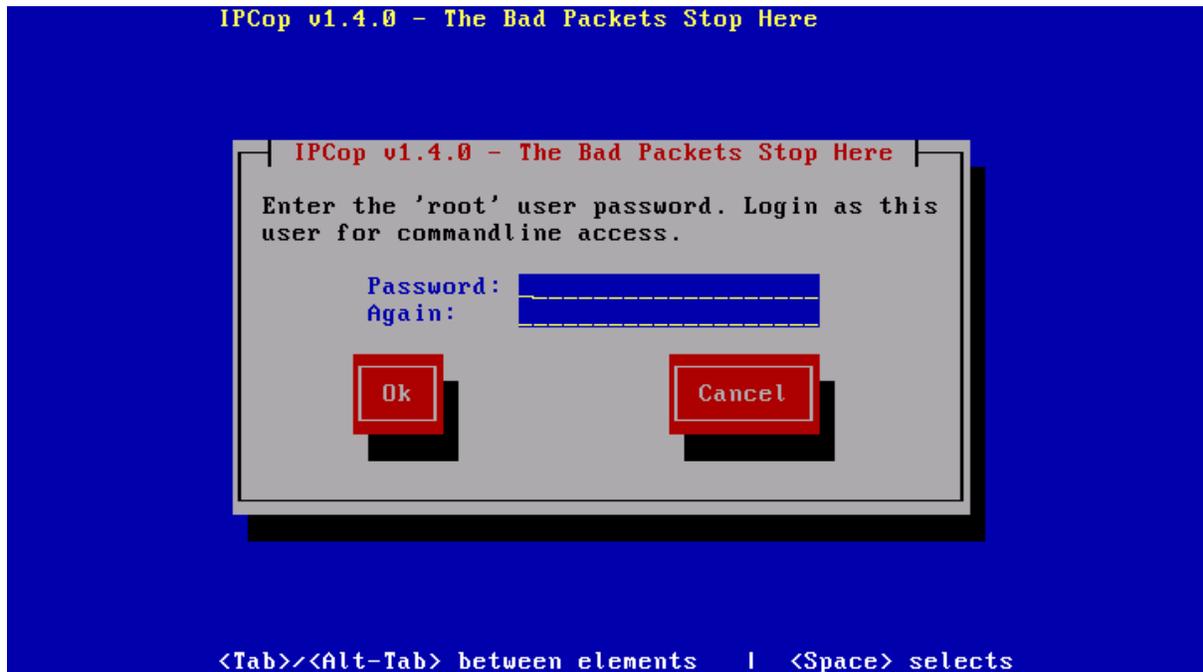
DHCP works by passing out leases on dynamic addresses that expire after a certain amount of time. Default lease time specifies the default lease time in minutes that DHCP will offer. After the default lease time, the client computer will attempt to ask for a new lease time for its acquired address. When the Max lease time has expired, the client computer is no longer allowed to ask for the acquired IP address, but the server may still pass out a lease on the acquired address.

Finally, the Domain name suffix allows you to specify a suffix that is automatically appended to DNS requests if the initial name can't be found. This will default to the domain name you set earlier. Many ISPs set up a domain name suffix, and then tell users to enter "mail", "news", or "www" to get to services. What really happens under the hood is that a DNS request is sent out for "mail" first. When the DNS servers indicate that they don't know an IP address

for mail, the next request is sent out with the domain name suffix appended, i.e. “mail.xxx.yyy.zzz.com” To make life easier, you may wish to add this suffix in the Domain name suffix line.

Unfortunately, space does not permit enough room on this line for some domain name suffixes. Please check the Administration Manual [http://www.ipcop.org/1.4.0/en/admin/html/services.html#services_dhcp] for another way to specify the suffix, which allows for a virtually unlimited length domain name suffix.

When you are done with the DHCP server configuration select the Ok button.



The next steps will set up IPCop’s root and web administrator passwords.

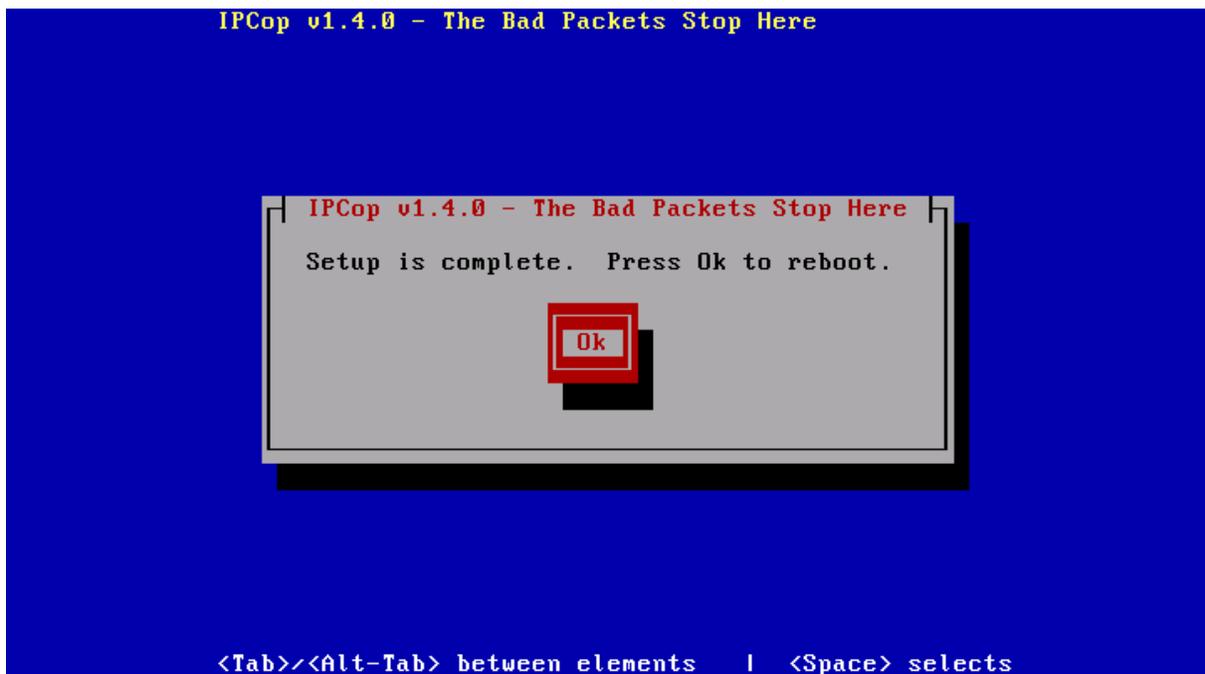
If you are familiar with Linux you may wish to login to the IPCop machine to carry maintenance tasks. The only user id configured is the “root” user. Enter the root password twice. Be careful, the root userid has the “keys to the kingdom” of your firewall. If someone gets its password they can cause all sorts of mischief. By default root is only allowed to log in via the local console, though.

Note that the cursor will not move when you are typing the passwords. The password will still be entered.



Finally, you will be prompted for your web admin password.

The IPCop web pages will prompt you for this user ID and password when you use the IPCop web pages to administer IPCop. Unlike the root user password, web browsers do not handle special characters in passwords very well. Limit your admin password to upper lower case alphanumeric characters.



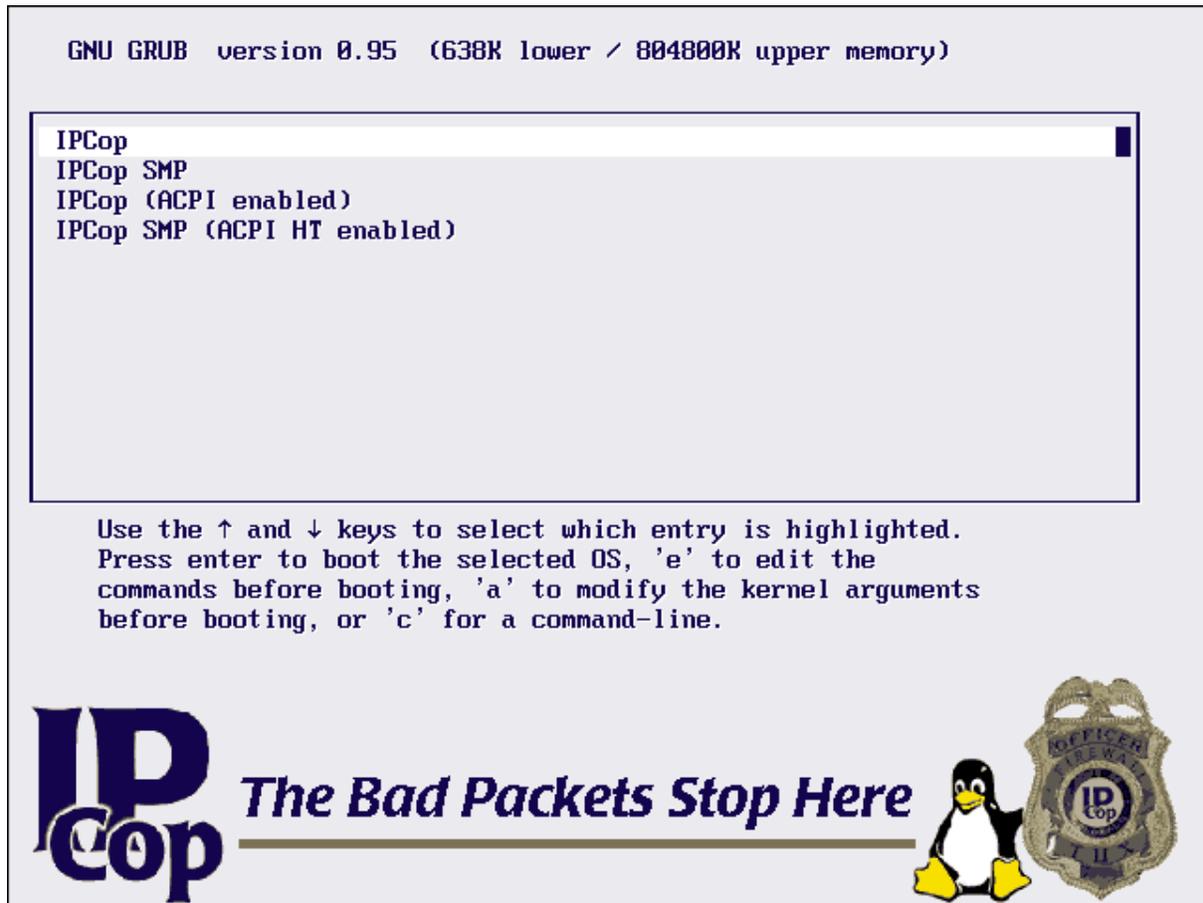
Congratulations!

You've completed your IPCop installation. Press Ok to reboot. After reboot is complete, you will undoubtedly need to perform some administrative tasks to complete you setup. For a complete description of how to administer IPCop, please check the Administration Manual [<http://www.ipcop.org/1.4.0/en/admin/html/>].

Chapter 4. After Installation

4.1. Choose Your Default Kernel Configuration

IPCop uses the GRUB boot loader to give you a choice of kernel configurations. During boot, the GRUB splash screen will appear.



GRUB Splash Screen

You will have 5 seconds to touch a keyboard key, before GRUB boots your default configuration. If you do not choose a configuration the default configuration, IPCop, will boot. If desired use the keyboard arrow keys to select a new kernel configuration.

If you want to use another configuration, make sure you can boot with it.

The Failsafe Configuration

The IPCop configuration is considered the *Failsafe* configuration. If you have a problem running another kernel configuration run the IPCop configuration.

GRUB's configurations are configured to be "sticky." In other words, GRUB will keep booting the last configuration chosen with the arrow keys, until the arrow keys are used to change its configuration.

There are four kernel configuration choices available:

IPCop This kernel configuration is suitable for single processor machines with motherboards that do not support the Advanced Configuration and Power Interface, ACPI, feature, see the ACPI discussion. This configuration is the most basic and should run on most processors and motherboards, even ones covered by the other kernel configurations.

IPCop SMP This kernel configuration is suitable for motherboards that have more than one processor, Symetric Multiprocessing. Choose this configuration if your mother board has more than 1 processor. If your processor chip(s) support hyperthreading you should probably be running the ACPI HT kernel.

IPCop (ACPI enabled) The Advanced Control and Power Interface, ACPI, allows IPCop to monitor key hardware metrics such as power and processor temprature. If necessary, IPCop, will power itself off to protect your processor and motherboard. ACPI requires an ACPI enabled chip set on your motherboard, ACPI aware BIOS, and the use of the “IPCop (ACPI enabled)” kernel. If you don’t know if your motherboard is ACPI enabled, check your motherboard or computer’s documentation. If you can’t find out, try booting one of the ACPI enabled kernels and check to see if the apci driver came up properly by logging in as root and typing:

```
# dmesg|grep ^ACPI:
```

Verify the ACPI reported no errors. If an error is reported, reboot and select another kernel configuration.

IPCop SMP (ACPI HT enabled) This kernel configuration supports processor chips with hyperthreading, HT, SMP and ACPI. Some Intel processors support hyperthreading, which is treated as an SMP, multiprocessing, configuration.

Once you have chosen an appropriate kernel configuration, press the **Enter** key to boot IPCop.

4.1.1. Changing the Default Configuration

“But I want IPCop to boot automatically!” The kernel configuration last chosen will be the default configuration, until changed.

4.2. Test Your Access to IPCop

Make sure you can access IPCop via a web browser. IPCop moves selected ports away from their standard numbers so that you can forward the well-known ports to real servers on your ORANGE network. The following examples assume you have set your GREEN network interface to 192.168.1.1. If not substitute the correct IP address. Verify that you can ping IPCop from a GREEN network machine. On Windows enter:

```
C:\ ping 192.168.1.1
```

On *nix and Macintosh OS X enter:

```
$ ping -n 192.168.1.1
```

IPCop's DNS proxy has not yet been enabled from its administration pages, so the ping command, above, deliberately stops ping from attempting to look up the fully qualified host name of the IPCop PC.

If ping works attempt to access your IPCop by opening a web browser to URL:

```
http://192.168.1.1:81/ [http://192.168.1.1:81/]
```

You should try the HTTPS, secure http port, next by attempting to access URL:

```
https://192.168.1.1:445/ [https://192.168.1.1:445/]
```

4.3. Optionally, Remove Unneeded Hardware

When you are satisfied with your IPCop installation, you can remove extra hardware on the IPCop PC: your video monitor and CD drive. You may want to leave your floppy disk drive in for backup purposes. If your BIOS permits, you can turn off keyboard detection and remove the keyboard, too.

If you remove the CD drive and/or floppy disk drive, remember to change your BIOS settings so the IPCop PC boots from its hard drive, first.

If you don't remove the floppy disk drive, so that you can use it for backup purposes, remember to change your BIOS settings so the IPCop PC never boots from the floppy drive.

Appendix A. Quick Home Networking Overview

More complete tutorials of home networking can be found on the web. A good place to start looking is the Linux Documentation Project Network Administrators Guide [<http://www.tldp.org/LDP/nag2/>].

IPCop requires Ethernet connections for your GREEN and optionally your ORANGE and BLUE network interfaces. This appendix will cover simple wiring and IP addressing well enough to get you through your IPCop installation.

A.1. Wiring

Unless you wind up with very old Ethernet cards, your Network Interface Cards or NICs will probably support one or two speeds on the network, 10 megabit, 10BaseT, or 100 megabit, 100BaseT. You can recognize these cards by the square connector on the back, called an RJ45 connector. If your cards have a different connector, check your manufacturer's web site.

Unless you have a very fast leased line connection to the Internet, 10BaseT cards will do for your NICs. Cable modems only transfer at 3 Megabits/sec. ADSL modems cannot go faster than 8 Megabits/sec.

You will be connecting the computers on your GREEN network to the IPCop computer on IPCop's internal GREEN NIC. If you have ORANGE or BLUE networks then these should be connected to the relevant NIC.

A.1.1. Only one computer on GREEN, BLUE or ORANGE

If there is only one computer on your network, all you will need is a single category 5 crossover cable. You can recognize a crossover cable by holding the transparent RJ45 connectors at each end next to each other. If the wires in the connector attach to different pins at either end of the cable, you have a cross over cable. Otherwise you have a straight through cable.

Connect IPCop and your computer to each other with the crossover cable. You have just set up your simple network.

A.1.2. Multiple Computer Networks

If you have more than the IPCop and a single computer on the same network, you will need to add another piece of hardware called a hub or a switch. The Ethernet protocol sends message packets to all computers on a network out of a single port, so all other computers on that network have to be able to see their packets, and be able to send packets to the other computers on that network.

If you have a hub or a switch, you will have to plug each computer on a network into the hub or switch via a straight through category 5 cables. Make sure each cable is a straight through cable by holding the transparent RJ45 connectors at each end of the cable next to each other. If the wires at each end attach to the same pins, you have a straight through cable.

A.2. IP Addressing

A.2.1. Format of an Address

An IP address consists of four numbers, ranging from 0 to 255, connected with dots, i.e. 192.168.1.1. This format is called a dotted IP address. Each computer on your networks needs a different IP address. Depending on your network configuration, IPCop needs between one and four different IP addresses.

A.2.2. Networks

An IP network consists of two or more computers with IP addresses in the same range. The network mask determines the ranges. Even though they are not mandatory any more, there are several default network masks based on the first number in the dotted IP address.

A.2.3. Network Address Classes

Class A networks' first numbers range from 1 to 126 (127 is special). These networks, with their default network mask of 255.0.0.0, allow over 16 million computers to be on the same network. Computers on the 4.x.y.z network, are on the same network. While computers on the 5.x.y.z network are on a different class A network. The IP address of x.0.0.0 designates the entire network and the IP address of x.255.255.255 designates a broadcast to every computer on the network.

Class B networks' first numbers range from 128 to 191. These networks with their default network mask of 255.255.0.0 allow over 65 thousand computers to be on the same network. Computers on the 190.4.y.z network, are on the same network. While computers on the 190.5.y.z network are on a different class B network. The IP address of x.y.0.0 designates the entire network and the IP address of x.y.255.255 designates a broadcast to every computer on the network.

Class C networks' first numbers range from 192 to 203. These networks with their default network mask of 255.255.255.0 allow over 250 computers to be on the same network. Computers on the 193.4.5.z network, are on the same network. While computers on the 193.4.6.z network are on a different class C network. The IP address of x.y.z.0 designates the entire network and the IP address of x.y.z.255 designates a broadcast to every computer on the network.

A.2.4. Private Address Ranges

Why should you care about this?

The powers that be have designated several IP address ranges as private in RFC1918 [<ftp://ftp.isi.edu/in-notes/rfc1918.txt>]. If packets addressed to or from one of these ranges leak out onto the Internet they will be discarded.

One of IPCop's features is Port Address Translation or PAT. Using this technique any conversations over the Internet will appear to originate from IPCop's RED network address. To help shield your GREEN, BLUE and ORANGE networks from malicious users, you should use private address ranges for your network(s). Remember, your GREEN, BLUE and ORANGE networks must have different network addresses.

The private address ranges are:

- 10.0.0.0 - A class A network. You can conceivably have over 16 million computers on this network.
- 172.16.0.0 through 172.31.0.0 - 16 class B networks. You can conceivably have over 64 thousand computers on each network.
- 192.168.0.0 through 192.168.255.0 - 256 class C networks. You can conceivably have over 250 computers on each network.

You can, if you wish, subdivide each network using a custom network mask. For example, if you wish to keep both your GREEN and ORANGE networks in the same private range, and you don't expect to ever need 32 thousand computers, you can use 172.16.0.0 with a network mask of 255.255.128 as your GREEN network and 172.16.128.0 with the same network mask as your ORANGE network. You will still have the ability to have over 32 thousand computers on each network.

Appendix B. Troubleshooting During The Install

B.1. Hidden Console Screens

During the install there are two hidden console screens that can be used for debugging. The screen you normally see during installation can be reached by pressing the **ALT-F1** key combination.

```
5/kernel/drivers/net/via-rhine.o.gz failed
/lib/modules/2.4.25/kernel/drivers/net/via-rhine.o.gz: insmod via-rhine failed
Running command: /sbin/modprobe winbond-840
/lib/modules/2.4.25/kernel/drivers/net/winbond-840.o.gz: init_module: No such de
vice
Hint: insmod errors can be caused by incorrect module parameters, including inva
lid IO or IRQ parameters.
    You may find more information in syslog or the output from dmesg
/lib/modules/2.4.25/kernel/drivers/net/winbond-840.o.gz: insmod /lib/modules/2.4
.25/kernel/drivers/net/winbond-840.o.gz failed
/lib/modules/2.4.25/kernel/drivers/net/winbond-840.o.gz: insmod winbond-840 fail
ed
Running command: /sbin/modprobe xircom_cb
Running command: /sbin/modprobe xircom_tulip_cb
/lib/modules/2.4.25/kernel/drivers/net/pcmcia/xircom_tulip_cb.o.gz: init_module:
No such device
Hint: insmod errors can be caused by incorrect module parameters, including inva
lid IO or IRQ parameters.
    You may find more information in syslog or the output from dmesg
/lib/modules/2.4.25/kernel/drivers/net/pcmcia/xircom_tulip_cb.o.gz: insmod /lib/
modules/2.4.25/kernel/drivers/net/pcmcia/xircom_tulip_cb.o.gz failed
/lib/modules/2.4.25/kernel/drivers/net/pcmcia/xircom_tulip_cb.o.gz: insmod xirco
m_tulip_cb failed
Running command: /etc/rc.d/rc.netaddress.down NOTGREEN
```

If you press **ALT-F2** you will see detail messages from the Linux commands run during the install.

After IPCop is installed on your hard drive, some late boot messages will appear if you press **ALT-F12**. If IPCop does not start up correctly, you may have a hardware error, so check this screen.

```
BusyBox v0.60.5 (2004.04.01-21:34+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# _
```

If you press **ALT-F3** you will be at a Linux command prompt.

During the first part of the install, until the full IPCop file system is built, the commands available at this prompt are extremely limited. Type

```
# help
```

for a list of shell built-in commands, and

```
# ls /bin
```

for a list of individual commands.

B.2. Loss of the Root Password

If you interrupt the installation or loose your root password, you can recover by booting IPCop in “single user” mode. To do this, attach a monitor and keyboard to your IPCop machine and reboot. During reboot, while the GRUB splash screen is displayed, press the **a** key. A long command line will appear with the cursor situated at the end. Press the **space** bar and type the word:

```
single
```

then press the **Enter** key. IPCop will boot and you will be placed at the command prompt, logged in as the root user. Enter:

```
sh-2.05b# passwd
```

You will be prompted to enter the root password, twice. Next reboot your machine by entering:

```
sh-2.05b# /usr/local/bin/ipcoprebirth
```

Appendix C. Creating Flash Based IPCop Systems

C.1. Why Run a Flash Based System?

Would you like to run your IPCop machine as a fan less network appliance? Many IPCop users remove their CD drives, floppy disks, keyboards and monitors from their IPCop firewalls. How about removing the hard drive?

Using IPCop's compact flash install, a compact flash card will simulate your hard drive. You will wind up with a very quiet machine, no disk drive noise and often no fan noise. Flash based systems are usually run on small "MiniITX" or other small footprint machines. Several manufacturers make machines that are great for use as IPCop machines, complete with multiple network cards.

Of course these machines tend to be more expensive than machines rescued from the dumpster.

Another popular reason to run from a small compact flash system is that these systems tend to be extremely portable. You can pack one along with your laptop and use it as a firewall in your hotel room.

You may be wondering about the viability of such a system, given the limits on the number of times a compact flash can be written to. IPCop changes its file system attributes so that the last file access time is not recorded on the flash's simulated hard drive. Logs and other temporary files are kept on a ram disk. The logs are compressed weekly, at shutdown and when the ram disk begins to fill up. Using this strategy, it has been estimated that a compact flash should be able to last 5 years.

C.2. Other CF Resources

If you're interested, visit the linITX.org [<http://www.linitx.org>] site. There are several topics on IPCop there.

The linITX.com [<http://linitx.com/support/download.php>] site usually has the latest flash image of IPCop available on its support pages.

C.3. Task Overview

Here is a quick overview of what you'll need to do to put IPCop on a compact flash:

- Obtain and become familiar with your target machine, compact flash memory, etc.
- Obtain a compact flash burner and become familiar with its use.
- If you're planning on creating your own compact flash image:
 - Install IPCop on a similar target machine or simulator using the distribution media.
 - Download the items in the CVS `ipcop/tools/mkflash` directory and transfer them to IPCop.
 - Log into IPCop as root and run the `mkflash.sh` script.
 - Transfer the `flash.img` file to another machine.

- Use a compact flash burner to transfer the flash image file to a compact flash device.
- Install the compact flash device and boot IPCop.
- Assign the Ethernet card drivers for your new machine.

C.4. CF Installation Steps

C.4.1. Obtain the Target Machine

You should obtain your target machine, first. Many of these machines do not have their compact flash drives on hard drive A. You will have to determine which disk drive the compact flash appears as.

Obviously, get a Compact Flash card. IPCop supports 128, 256 and 512 MByte compact flash cards as well as 1 GByte cards. The larger the compact flash you use, the more logs can be retained.

The flash version of IPCop uses a 64 MByte ram disk to hold logs until they are compressed and moved to your compact flash for long-term storage. The ram disk is also used for the web proxy cache. Determine how much memory you will need to hold the ram disk and IPCop run time memory. 128 MByte is probably enough.

Since this is an Open Source Project, unaffiliated with any commercial entity, we will not recommend a computer. There have been some discussions on this topic on the IPCop mailing lists. Please go to the [IPCop Mailing Lists Page](http://www.ipcop.org/cgi-bin/twiki/view/PCop/PCopMailingLists) [<http://www.ipcop.org/cgi-bin/twiki/view/PCop/PCopMailingLists>] and search the archives for discussions on compact flash installations.

If you are going to use an image from the Internet download it and skip to the discussion of writing the compact flash, otherwise continue with the discussion of installing IPCop on a staging machine installing IPCop on a staging machine.

C.4.2. Install IPCop On a Staging Machine

The next thing that's required is a running IPCop system with at least a 500 MByte hard drive. You won't need a stand-alone computer for this. Bochs [<http://bochs.sourceforge.net/>], an x86 simulator is Open Source. There is a discussion of how to install Bochs for use with IPCop at the Bochs HOWTO [<http://www.ipcop.org/cgi-bin/twiki/view/PCop/PCopBochsv01>] page. Other simulators may be used as well, some commercial. Of course, there's nothing keeping you from using a real computer.

While an existing IPCop machine can be used, all logs should be deleted. **mkflash.sh** will try to copy all the existing logs and **snort** cache files to the flash image it's creating. This will easily fill your flash image. Remember, the log and **snort** cache files will be on a separate ram disk, while your compact flash based system is running.

Install IPCop on your staging computer. A CD-ROM install is probably the easiest since most simulators allow an ISO file to be used directly.

C.4.3. Get **mkflash.sh** and Associated Files

The files necessary to create a compact flash image are kept in the IPCop CVS archive on SourceForge.net. To get them, go to the [IPCop CVS view page for `mkflash`](http://cvs.sourceforge.net/viewcvs.py/ipcop/ipcop/tools/mkflash/?only_with_tag=) [http://cvs.sourceforge.net/viewcvs.py/ipcop/ipcop/tools/mkflash/?only_with_tag=] and download the files displayed using your web browser.

C.4.4. Upload **mkflash.sh**

Make sure you have enabled **ssh** on your staging machine. Transfer the files you've just downloaded to root's home directory on the staging machine. Check the IPCop Administration Manual [<http://www.ipcop.org/1.4.0/en/admin/html/system.html#ssh>] for a discussion on how to enable **ssh** and transfer files to IPCop.

C.4.5. Run mkflash.sh

Log into the staging machine as root. The `mkflash.sh` shell script will not have been marked as executable when you transferred it to the staging machine. To make it executable, issue:

```
# chmod u+x mkflash.sh
```

Now run **mkflash.sh**. You must specify the size of your compact flash and the hard drive you compact flash will wind up on as parameters on the command line. For example, to create a 128 MByte image that will wind up as `hdc`, enter:

```
# ./mkflash.sh 128 hdc
```

When **mkflash.sh** completes, a file named `/tmp/nnnflash.img` will be on your staging machine, where `nnn` is the flash size. Use **scp** or **pscp** on Windows to transfer the `nnnflash.img` file to another computer to write your compact flash.

C.4.6. Write the Compact Flash

Connect your compact flash writer to your workstation and insert your compact flash.

C.4.6.1. Writing a Compact Flash Under *nix

If your workstation is running *nix, you will have to determine which physical hard drive your compact flash writer appears as.

Issue a **df** to see which currently connected physical devices are mounted and contain file systems. *Do not use any of these as a target for the **dd**, below.* For example, if you see several file systems on `/dev/hdan` do not use `/dev/hda` as an output target of the **dd** command.

Try mounting other physical disks to see what your writer appears as, including `/dev/hdn1` and `/dev/sdn1`. Once you've figured out its address **umount** the device.

Issue the following command:

```
# dd if=nnnflash.img of=/dev/hdn
```

The creation of your compact flash may take a few minutes.

Once the **dd** returns, **mount** /dev/hdn1 and verify that the first IPCop partition is visible by issuing an **ls** command. Then **umount** the disk.

C.4.6.2. Writing a Compact Flash Under Windows

There are several programs available under Windows for creating a compact flash image. One such is physdiskwrite [<http://m0n0.ch/wall/physdiskwrite.php>].

Use such a program to write your compact flash. This may take a while.

C.4.7. Install Your New Image and Boot

You're finally ready to plug your compact flash into your target machine. Boot it. If you get error messages about the kernel being unable to find the root file system, your disk drive does not match the one the compact flash image was created to use.

C.4.8. Run the Setup Command

Unfortunately, the NIC and/or modem configuration on your target machine is probably different than the staging machine. If you've downloaded your compact flash image from the Internet the same will be true.

To fix problems like this and to reset your passwords, log in to your target machine as root. Run the **setup** command to change IPCop's configuration as desired.

C.5. Backing Up Your Compact Flash Using ssh

The normal IPCop backup facilities are available when running from a compact flash. In addition, it may be worthwhile for you to save the entire compact flash image as an `.img` file. This way, in case you want to create a new compact flash with your entire configuration on it, you can use the `.img` file to create it.

Turn on ssh via the web page [<http://www.ipcop.org/1.4.0/en/admin/html/system.html#ssh>]. Then from a Unix or Linux machine or Cygwin on a Windows machine issue:

```
$ ssh -p 222 root@192.168.1.1 "dd if=/dev/harddisk >backup.img"
```

This command utilizes **ssh**'s ability to run commands submitted at the end of the command line. In this case the command sequence uses the **dd** command to copy the entire physical compact flash device and then put the output into a file on your local computer.

Appendix D. GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

D.1. 0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

D.2. 1. Applicability and Definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

D.3. 2. Verbatim Copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

D.4. 3. Copying In Quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

D.5. 4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. In any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made ‘by’) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

D.6. 5. Combining Documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements.”

D.7. 6. Collections of Documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

D.8. 7. Aggregation With Independent Works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

D.9. 8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

D.10. 9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

D.11. 10. Future Revisions of This License

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See the GNU Free Documentation License [<http://www.gnu.org/licenses/licenses.html#FDL>] web site.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

D.12. ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright© YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License [<http://www.gnu.org/licenses/gpl.html>] to permit their use in free software.