

The Whistle Commander ISP Guide

Whistle Commander 1.0



Whistle Communications Corp.
110 Marsh Drive
Foster City, CA 94404
U.S.A.

Important Notice

© Copyright 1997 Whistle Communications Corporation

All rights reserved. First edition printed 1997. Printed in the United States.

Under the copyright laws, neither the documentation nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part.

No liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Macintosh is a registered trademark of Apple Computer, Inc.; UNIX is a registered trademark of AT&T; Internet Explorer is a trademark and Microsoft and Windows are registered trademarks of Microsoft Corporation; Netscape Navigator and Netscape are registered trademarks of Netscape Communications, Inc.

Other product and company names herein may be the trademarks of their respective owners.



Table of Contents

Chapter 1. Introduction to Whistle Commander. 1-1

Overview 1-1

The Auto-Configuration Process. 1-1

How Whistle Commander Works. 1-2

Using This Guide 1-2

Chapter 2. Installing Whistle Commander 2-1

System Requirements 2-1

The Installation Procedure. 2-2

Whistle Commander Installation Tests. 2-3

Security Considerations 2-6

Chapter 3. Using Whistle Commander 3-1

Accessing Whistle Commander 3-1

Creating a New Account 3-3

Viewing Accounts 3-4

Editing Accounts 3-5

Account Fields 3-5

Lockdown Fields 3-27

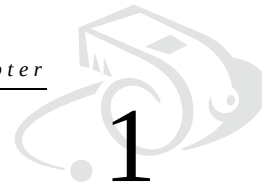
Setting Up Default Values 3-28

Sample Configuration Files. 3-29

 Sample Globals File 3-29

Table of Contents

Sample Defaults File	3-29
----------------------------	------



Introduction to Whistle Commander

Overview

Whistle Commander provides you, the Internet service provider (ISP), with a convenient way to set up accounts for your InterJet customers. You run the Whistle Commander software at your site to specify the account information, and then your InterJet customer runs the auto-configuration process to download this information to the InterJet. The auto-configuration process benefits both you and your customer in the following ways:

- Provides an easy-to-use setup mechanism for end users
- Prevents end users from entering incorrect settings into their InterJets
- Gives you control over the settings installed onto the InterJet
- Reduces your overhead for “bench configuring” a piece of equipment



Note: Whistle Commander helps you to set up InterJet accounts for auto-configuration. You must first configure DNS, PPP accounts, routing, and so on at your site—Whistle Commander does not configure any of these things for you.

The Auto-Configuration Process

Whistle Commander makes it easy for your InterJet customer to get up and running on the Internet. Because you use the Whistle Commander software to program all of the detailed settings needed to connect to the InterJet, these settings are ready for the InterJet to download when it dials in for auto-configuration. Using the InterJet's built-in DCHP (Dynamic Host Configuration Protocol) server, your customer can set up the InterJet and client machines without ever entering a single IP address.

The following steps outline the auto-configuration process to help you to understand the context in which Whistle Commander works.

1. You get an order for an InterJet account.
2. You obtain all the information necessary to create the new account.

3. You start Whistle Commander administration interface in a Web browser.
4. Using Whistle Commander administration interface, you create a new account, fill in the pertinent information, and submit the form, as described in this guide.
5. Whistle Commander provides a 24-digit registration ID and an InterJet Setup Sheet for you to fax to the customer; this sheet has all of the information your customer needs to remotely configure the InterJet.
6. The customer receives an InterJet and the InterJet Setup Sheet. The customer plugs in the InterJet and enters the 24-digit registration ID and phone number, as provided on the Setup Sheet.
7. The InterJet automatically dials into the ISP, downloads the configuration information from Whistle Commander (through HTTP), including its WAN static IP address, WAN dial-up login ID and phone number, domain name server, mail server, and so on.
8. The InterJet uses the information to configure itself, then dials out to the ISP POP (Point of Presence). Once the WAN connection is established, the InterJet is visible to the Internet.

How Whistle Commander Works

The Whistle Commander software is implemented as Perl `cgi` scripts running within the context of a Web server. You use a Web browser to access Web pages that you can use to create, edit, delete, and examine accounts. The account information is stored in a `gdbm` database, and all access to the database is through the Perl scripts. For auto-configuration, the InterJet connects to the Web server and runs one of the `cgi` scripts to download the account information using Whistle's Auto-Configuration Language (ACL). A compiled program, `regid`, encodes and decodes the registration IDs.

Using This Guide

- This chapter contains a general overview of Whistle Commander and a description of how the software is implemented.
- Chapter 2 explains how to install and test Whistle Commander software.
- Chapter 3 describes how to provide the information that Whistle Commander needs to auto-configure InterJets.



Installing Whistle Commander

The Whistle Commander software is available from the Whistle FTP site. You must download it and uncompress and untar it to the location you choose as your Whistle Commander system.



Note: You should install your Whistle Commander software on a computer whose IP address is unlikely to change. Because the IP address of the Whistle Commander system is encoded in the registration ID, if the computer is moved to another IP address, all of the currently issued registration IDs become invalid. If you do move the Commander system, generate new registration IDs and notify customers of the change.

System Requirements

To run Whistle Commander, you must have the following installed and operational on a UNIX system:

- Dial-up PPP access to the Whistle Commander system
- A C compiler
- A GNU gdbm package
- Perl 5.003 or later with gdbm support
- A Web server capable of running `cgi` scripts
- A Web browser. Use one of the following Web browsers for Macintosh, Windows, and UNIX computers:
 - Netscape Navigator 2.02
 - Netscape Navigator 3.x
 - Netscape Navigator 4.x

For a Windows computer, you can also use Internet Explorer 4.0.

The Installation Procedure

To install Whistle Commander, use the following steps:

1. Download the Whistle Commander software from the Whistle FTP site:
`ftp://ftp.whistle.com`
The login ID, password, and location information is provided on a separate sheet of paper in your InterJet evaluation kit.
2. Uncompress and untar the image after downloading it from the server. To do this, use the following `zcat` command:
`zcat commander-1.0.tar.Z | tar xvf -`
(Note that the file name reflects the current version number.)
3. From the directory in which you untarred the image, enter the following command:
`cp config.orig config`
This creates a new file, `config`, in your top-level directory.
4. Use a text editor to edit the values in the `config` file to reflect your system setup, as follows:
 - Set the shell variable `PERL5PROG` to the full path name of the `perl5` executable on your system.
 - Set `HTTPBASEDIR` to the base directory of your Web site file directory. This should be where you store your `.html` files.

The following is a sample `config` file:

```
#
# PERL5PROG = Path name of the Perl 5 executable
#
PERL5PROG=/usr/local/bin/perl
#
# HTTPBASEDIR = Base dir for the top-level Web server dir
#
HTTPBASEDIR=/usr/local/etc/httpd/htdocs
```

5. Build the source code for the Whistle Commander software. To do this, enter the following command:
`make all`

This command descends into the `src` directory and builds the `regid` program. The command returns very quickly.

6. Install the Whistle Commander software. To do this, enter the following command:

```
make install
```

This copies the installation to your Web server at the location
`${HTTPBASEDIR}/whistle/interjet`.

7. Use a text editor to edit the values in the configuration files to reflect the defaults that are appropriate for a new account at your site. These files are:

```
${HTTPBASEDIR}/whistle/interjet/admin/Databases/defaults
```

```
${HTTPBASEDIR}/whistle/interjet/admin/Databases/globals
```

The `defaults` file contains the default values that are automatically entered in the editable fields of any new account that you create using Whistle Commander. The `globals` file contains the dial-up number that all InterJets use to reach Whistle Commander for auto-configuration. This number is included on the InterJet Setup Sheet, which you fax to the customer. The `globals` file should also contain the IP address of the Commander system, which is encoded in the registration ID.

Samples of these files are shown in the section "Sample Configuration Files" on page 3-29.

8. Test the installation as described in the following section.

Whistle Commander Installation Tests

You must test Whistle Commander to make sure that it has been downloaded and installed correctly. It is recommended that you perform all of the following tests.

1. To ensure Perl is working properly, run the test programs in the Perl source directory. To run the tests:
 - a. Change directory to the Perl source directory and enter the following command:

```
make test
```

This command runs a number of tests; each test is shown by name and marked ok when it passes. All tests must pass, and the final paragraph of the returned text should include the phrase `All tests successful`.

- b. Test the version by entering the command:

```
perl -v
```

This command should return a version number of 5.003 or later.
 - c. Test that GNU gdbm is supported by entering the command:

```
perl -e "require GDBM_File"
```

This command should return nothing; if gdbm is not supported, the command returns an error message.
2. Run the `regid` program to test the encode and decode modes. To do this:
 - a. From the Whistle Commander source directory, enter the following command:

```
% ./src/regid -e 10 127.0.0.1
```

You should see the following `regid` output:

```
611404002067251531420038
```
 - b. Now run the decode function:

```
% ./src/regid -d 611404002067251531420038
```

You should see following output:

```
10 127.0.0.1
```
3. Go to the Whistle Commander home page by typing the following URL in a Web browser:

```
http://<commander_hostname>/whistle/interjet/admin/index.cgi
```

You should see the initial page in your browser, which is the `index.cgi` file. If you do not see this page, it could indicate a misconfiguration in the Web server setup for either detecting an `index.cgi` file or running `cgi` scripts within the directory hierarchy.

 - If your Web browser displays a listing of the files in the `/whistle/interjet/admin` directory, then your Web server is not set up to recognize `index.cgi` as a valid directory index file. Configurations vary from server to server; on the Apache server, look for the directive `DirectoryIndex` in the configuration files. It should look like this:

```
DirectoryIndex index.html index.cgi index.htm
```

If necessary, modify the configuration file and restart your Web server.

- If your Web browser does not properly execute the `index.cgi` file, you must enable this capability. For the Apache Web server, this is set in the `access.conf` file. Specify the `Options` directive for the top-level directory as either `ExecCGI` or `All`. Change the file and restart your Web server to fix this problem.
4. Create a new account using Whistle Commander, as described in the section "Creating a New Account" on page 3-3. When you have submitted the new account information, the system should generate a registration ID for the new account. View or edit the new account, and make a note of the new registration ID number.
 5. Test the `autoconfig.cgi` script, which is the script executed by the InterJet when it tries to configure itself remotely. You must pass two parameters to the script to get back valid configuration information: a valid registration ID and the Ethernet hardware address of the InterJet, also called the MAC address. The address need not be a valid address. Run this script from your Web browser by going to the following URL:
`http://<commander_hostname>/whistle/interjet/
autoconfig.cgi?regid=XXXX&macaddr=10`
For `<commander_hostname>`, substitute the fully qualified domain name (FQDN) of your Whistle Commander server.
For `XXXX`, substitute the registration ID number generated when you created the account in Step 4.
If the `autoconfig.cgi` script is functioning properly, you should not get any server errors, and you should see a screen of Auto-Configuration Language (ACL).
 6. Return the Web browser to the Whistle Commander Accounts List page. Select and edit the new account, as described in the section "Editing Accounts" on page 3-5. Clear the MAC address from the `AutoConfig Mode` field and click **Submit**. This allows the account to be used for further testing with an InterJet.



Important: Make sure there is a PPP login to your dial-up port with a login name of `IAConfig` and a password of `IAConfig`. The InterJet uses this login name and password when remotely configuring itself. For more information, refer to the section "Security Considerations" on page 2-6.

7. Auto-configure an InterJet using the newly created registration ID and the dial-up phone number. The auto-configuration process is described in the Installation/Configuration section of *The InterJet Administrator's Guide*.

Security Considerations

Since the auto-configuration uses a widely known login name and password, you should limit the `IAConfig` account to only route to the Whistle Commander system, or provide an isolated system or network. In addition, to protect your Whistle Commander database, use a Web server security mechanism to protect the administration pages. For the Apache Web server, put an `.htaccess` file in the `${HTTPBASEDIR}/whistle/interjet/admin` directory. Refer to the Web server's documentation for information on `.htaccess` files and how to set up passwords.



Important: Do not put an `.htaccess` file in the directory `${HTTPBASEDIR}/whistle/interjet`. This file would prevent the InterJet from running the `autoconfig.cgi` script in that directory.

You can use the following methods to secure the `IAConfig` account:

- Limit connections to three minutes. Auto-configuration takes less than a minute, so there is no need to stay connected longer.
- Set up filters for the `IAConfig` account's IP address so that it can only access the Commander system. You should make sure this account cannot access the Internet or other servers.



Using Whistle Commander

You use Whistle Commander to create and edit accounts for each of your InterJet customers. This chapter describes:

- How to access Whistle Commander
- How to control the display of accounts so that it is easy to find and select the account you want
- How to create a new account, including how to set up default values that are appropriate for your site
- How to use the various read-only views of accounts and generate the InterJet Setup Sheet for your customers
- How to edit an existing account to modify the information in it

Accessing Whistle Commander

Bring up Whistle Commander in a Web browser by typing in the URL where you installed it. For example, type in the location:

`http://<commander_hostname>/whistle/interjet/admin/index.cgi`

Click the Whistle logo to get to the Accounts List page, shown in Figure 3-1.



Figure 3-1 The Accounts List page

The center part of this page displays a list of all the accounts you have created.

You can scroll to a particular account by typing in the first few letters of the organization name into the text box beneath the list and pressing the ENTER key.

If you have a large number of accounts, you can filter the list to show a smaller subset, making it easier to find a specific account. Specify the filtering criteria in the fields below the list. When you have made your selections, click **OK** to display the new filtered list.

You can select an account from the list and use the buttons on the right to edit it, view it in various ways, or delete it (after a confirmation). The button at the top right allows you to create a new account.

Creating a New Account

Click **New Account** on the Accounts List page to create a new account. The New/Edit Account page appears, as shown in Figure 3-2.

Edit Account for "Andersen Konditorei AB"

Auto-Configuration Status

Regid: 5946 0400 2843 4295 4242 0000 Last Attempt: never

Auto-Config Mode: ☐ Disabled

☐ Allowed ONLY from ethernet address: [unknown]
 (If 'unknown' or blank, the ethernet hardware address will be gleaned upon next successful config and enforced for subsequent attempts.)

☐ Allowed from any EN HW address.

Lockdown: ☐ Local admin cannot alter settings of fields defined in "Database/lockdown"

Organization Info

Company Name: [Andersen Konditorei AB]

Contact: [] Telephone #: []

Email: [] Fax #: []

Address 1: []

Address 2: []

City: [] State/Province: []

Zip/Postal Code: [] Country: []

Domain Name Service (DNS)

Figure 3-2 The New/Edit Account page

The page is divided into a number of sections; an index of sections appears on the left side of the page. Click the name of a section to scroll directly to that section.

When the page first appears, default values are filled in for some fields. Refer to the section "Setting Up Default Values" on page 3-28 for information on how to specify defaults that are appropriate for your site. You must provide specific (non-default) values for the following fields:

- Company name
- InterJet's domain

➤ PPP information

A description of each field is given in Table 3-1 on page 3-5.

When you have finished specifying the information, click the **OK** button at the bottom of the page to create the new account. Click **Cancel** to discard the changes you have made and return to the previous page without creating the account.



Important: When you have created an account, use the **View Setup Sheet** button to display and print the InterJet Setup Sheet, which you must send to the customer with the InterJet. The account information on the Setup Sheet allows the customer to start the auto-configuration process.

Viewing Accounts

There are three **View** buttons on the Accounts List page that show you three different views of the selected account. These views show only the current status of the account. You cannot edit the information in the views. To modify any of the account information, use the **Edit Account** button, as described in the section "Editing Accounts" on page 3-5.

➤ **View Setup Sheet**

This button shows you the InterJet Setup Sheet, which is a read-only summary of the selected account. It includes all the information the customer needs (such as the registration ID number) to start the auto-configuration of the InterJet. Print this page to send or fax it to the customer.

➤ **View Account**

This button shows you a read-only version of the current settings for the selected account. This view allows you to print the account information if you are using a browser that does not print HTML forms well.

➤ **View Config Output**

This button shows you the Auto-Configuration Language file that is generated for the selected account based on the profile you have created. Use this view for troubleshooting customer problems. When a customer encounters a dialog box with the message `error on line n`, the line number refers to a line in this file. Use this view to locate the error, then use the **Edit Account** button at the top or bottom of the screen to correct the problem by modifying the account information. The **Accounts** button returns you to the Accounts List page.

Editing Accounts

To modify information in an account, select the account on the Accounts List page and click **Edit Account**. The New/Edit Account page appears. This page is similar to the page used for creating new accounts, except that the current account information is shown. The fields that can be modified are described in Table 3-1 below.

When you have finished specifying the information, click the **OK** button at the bottom of the page to modify the account using the new information. Click **Cancel** to discard the changes you have made and return to the previous page without modifying the account.

Account Fields

Table 3-1 describes each field that you can specify for an account. The fields are described in the order in which they appear on the New/Edit Account page.

Table 3-1 Account Fields

Section: Auto-Configuration Status	
Regid	
Description	The unique 24-digit registration ID for this InterJet account. Generated by Commander when new account profile is created, it encodes the IP address of the Commander system.
InterJet GUI	Entered using the InterJet's keypad to initiate auto-configuration and displayed on the LCD InterJet Setup screen (main menu #1, option #1).
Note	This field is shown only for existing accounts, not when you are creating a new account. The field is not editable.
Last Attempt	
Description	Time stamp of last attempt to auto-configure this account (if ever), in YYMMDD HHMMSS format.
InterJet GUI	Displayed on the InterJet's LCD InterJet Setup screen (main menu #1).

Table 3-1 Account Fields (continued)

Note	This field is shown only for existing accounts, not when you are creating a new account. The field is not editable.
Last Result	
Description	String describing the result of the last attempt at auto-configuration, either OK- Sent ACL version X or a descriptive reason for failure.
InterJet GUI	If auto-configuration fails, the InterJet displays a similar message on the LCD. After an attempted auto-configuration, the InterJet displays OK or FAIL on the LCD InterJet Setup screen (main menu #1).
Note	This field is shown only for existing accounts that have previously attempted auto-configuration. The field is not editable.
ACL Requested	
Description	Version of the Auto-Configuration Language requested by the InterJet upon last auto-configuration. This is determined by the WhistleWare version running on the InterJet.
Note	This field is shown only for existing accounts that have previously attempted auto-configuration. The field is not editable.
WhistleWare	
Description	Version of WhistleWare that the InterJet was running at the time of the most recent auto-configuration.
InterJet GUI	Displayed on the InterJet's LCD System Settings screen (main menu #4). Also displayed on the System Agent's Information page. The local administrator can update the WhistleWare software using the System Agent's Maintenance Upgrade page.
Note	This field is shown only for existing accounts that have previously attempted auto-configuration. The field is not editable.

Table 3-1 Account Fields (continued)

Auto-Conf Mode	
Description	The radio buttons in this section determine which InterJets (if any) are allowed to auto-configure using this profile. Disabled: This option prevents the account from being auto-configured from an InterJet. This is intended to be used when an account is not ready to be auto-configured because the setup information is incomplete, or when an account is <i>deprecated</i> (no longer used or needed but not deleted from the database). Allowed ONLY from ethernet address: This is the default setting for an account. It provides a level of security to the configuration information. After an InterJet successfully auto-configures, the InterJet's primary Ethernet hardware address (MAC address) is stored into the database. Subsequent auto-configurations from that InterJet succeed, while auto-configurations from a different InterJet fail, since the Ethernet hardware address is different. Allowed from any EN HW address: This option is intended for test or demo accounts where more than one InterJet needs to auto-configure using the same account information.
Lockdown	
Description	This check box determines whether certain fields in the InterJet's administrative pages are locked. When fields are locked, they are not locally editable. Note: Lockdown is a feature of WhistleWare 2.x, and is not supported in WhistleWare 1.x. If the lockdown feature is enabled, the auto-configuration of a WhistleWare 1.x InterJet will fail. The set of fields that are locked when lockdown is enabled is predetermined. All lockable fields are either locked or unlocked—fields cannot be locked individually. A complete list of lockable fields is given in the section "Lockdown Fields" on page 3-27.

Table 3-1 Account Fields (continued)

InterJet GUI	If lockdown is enabled, the locked field values are displayed but not editable in the InterJet's administrative pages. The local administrator cannot modify the values of locked fields, and must contact the ISP if any adjustments are required. If lockdown is not enabled, all fields are editable by a local administrator with the proper privileges. The local administrator can alter values set during auto-configuration.
Section: Organization Info	
Company Name Contact Telephone Fax Email Address 1 Address 2 City State/Province Zip/Postal Code Country	
Description	These text fields specify the user contact details. This information is downloaded to the InterJet to be used in the creation of the user's initial Web pages. The Company Name field is required and is the default primary look-up key in Whistle Commander for subsequent modifications to the account.
InterJet GUI	WhistleWare 1.x: The values from these fields are displayed and editable on the Personnel Organization page. WhistleWare 2.x: The values from these fields are shown but not editable from the Personnel Organization page. A local version of the information is displayed and editable on the Webmaster Contact Information page.
Section: Domain Name Service (DNS)	
InterJet GUI	The DNS field values are shown on the System Agent's Network General page.

Table 3-1 Account Fields (continued)

InterJet's Domain	
Description	Enter the domain for which the InterJet will be the primary DNS server. You should also run a name server for this domain, so that the rest of the Internet can access the InterJet's external services by name. If the InterJet has a full-time connection, your name server can be secondary to the InterJet and get zone transfers from the InterJet. If the InterJet is not always connected, your name server should be primary for the local domain and have appropriate DNS resource records for the InterJet's external services—for example, MX records for mail delivery.
Forwarding NS 1 Forwarding NS 2	
Description	<i>Optional:</i> Enter the IP addresses of the ISP forwarding name servers. If specified, the InterJet uses these name servers as an initial look-up point for domain names outside its domain. If not specified, the InterJet uses the root name servers instead.
MX Backup 1 MX Backup 2	
Description	Enter the fully qualified domain name (FQDN) of the ISP backup mail servers (corresponding to any servers listed on the right side of DNS MX resource records for the InterJet's domain). These servers should be set up to accept mail for the InterJet's domain when the InterJet is offline. This mail should be delivered to the InterJet via SMTP when these servers process their queues, or when the InterJet uses ETRN or finger to poll them. These fields are used only in WhistleWare 2.x, and only for a full-time connection. If the InterJet uses WhistleWare 1.x or dial-on-demand, the backup mail server for ETRN is determined dynamically.

Table 3-1 Account Fields (continued)

Secondary NS 1 Secondary NS 2	
Description	Enter the fully qualified domain name (FQDN) of up to two ISP secondary name servers for the InterJet's domain. It is recommended that you specify at least one secondary name server at your site for full-time connections. If a name server is not specified here, it cannot receive zone transfers from the InterJet for publicly known name mappings.
Section: Microsoft Filesharing (SMB)	
Workgroup	
Description	Specifies the Windows workgroup setting for the InterJet. Windows users can find the InterJet in this workgroup by browsing their Network Neighborhood. The InterJet's Windows file sharing is always enabled and can be ignored if the client network has no Windows computers. If this field is left blank, the InterJet's workgroup setting is not altered.
InterJet GUI	This field value is displayed and editable on the System Agent's Network General page. On the InterJet's LCD, the workgroup is displayed on the Network Settings/ Show Sharing Info screen (main menu #3, option #3 or #4).
Section: Internal LAN (secured)	
LAN IP Address Netmask	
Description	Specify the InterJet IP address on its LAN interface (secured Office Ethernet) and the range of valid IP addresses on this network. A typical class C network would use a netmask of 255.255.255.0, also expressible as /24, meaning that the netmask is 24 bits wide.

Table 3-1 Account Fields (continued)

InterJet GUI	On the InterJet's LCD, these values are displayed and can be set on the Network Settings screen (main menu #3, option #1). The network address and netmask can be examined and set by editing the Office Ethernet network entry from the System Agent's Network View page. Then, the InterJet's IP address on that network can be set by editing the InterJet's machine entry.
Enable DHCP Dynamic Range	
Description	Enable DHCP on this net Select the check box to enable DHCP (Dynamic Host Configuration Protocol). When enabled, the DHCP server responds to requests from DHCP clients (such as Windows 95 and Macintosh systems) by dynamically assigning IP addresses, rather than requiring that static IP addresses be assigned. This is the preferred method. DHCP dynamic range Sets the range available for DHCP allocation relative to the network address. A customer might want some number of static addresses available for Windows 3.1 systems, printers, and other non-DHCP-capable devices. The default is to use the top half of the available network addresses for dynamic assignment to DHCP clients.
InterJet GUI	The DHCP server can be enabled or disabled from the InterJet's LCD Network Settings screen (main menu #3, option #2 or #3). These and other DHCP parameters can be set by editing the Office Ethernet network entry in the System Agent's Network View page.

Table 3-1 Account Fields (continued)

Firewall	
Description	Enable Address Translation Select the check box to enable address translation. When enabled, the InterJet maps internal IP addresses to its own WAN IP address when making external connections. This means that the source address on outgoing packets is rewritten so that, from the outside world, it appears as if the entire internal network is a single host, namely the InterJet. Address translation is necessary when you are using an unroutable internal IP range such as 192.168.1.0/24, although you can also use address translation with a real (routable) IP range. When address translation is disabled, the InterJet behaves as a normal router, with the source address of outgoing packets unmodified. You must have a real IP address range for this to work correctly; that is, there must be a route to the internal network if address translation is not used. Note: If address translation is disabled, the InterJet's packet filtering (firewall) does not allow connections to internal machines to be initiated from the outside (except when allowed for active FTP). Allow active FTP from LAN Select the check box to allow active FTP downloads from the Internet to the InterJet's internal LAN. For security reasons, Whistle recommends this be OFF by default. It can be enabled by the local administrator if necessary to connect to FTP servers not supporting passive FTP, or if LAN clients are using an FTP application that does not support passive mode.
InterJet GUI	The address translation and active FTP settings are displayed and editable on the System Agent's Network General page.

Table 3-1 Account Fields (continued)

Section: Perimeter LAN (publicly accessible)	
Perimeter IP Address Netmask	
Description	Specify the InterJet's IP address on its Perimeter network interface (publicly accessible Ethernet) and the range of valid IP addresses on this network. Because customers will likely have fewer public servers than internal clients, the netmask on this network can be something like 255.255.255.240 (or /28), providing 13 usable addresses on this network in addition to the network, broadcast, and InterJet addresses. If left blank, Commander does not attempt to configure the InterJet's Perimeter network. If configured, the Perimeter network addresses MUST be routable, as they are intended for publicly accessible servers. If the account profile attempts to configure the Perimeter network but the InterJet does not have the required hardware, auto-configuration fails with an appropriate error message on the InterJet's LCD and the profile's Last Result field. Note: When the Perimeter network is configured, all of the InterJet's public services (SMTP, Web, and FTP servers, if enabled) are bound to the InterJet's Perimeter IP address, which is normally the same as the WAN IP address. When the Perimeter network is not configured, the public services are bound to the InterJet's WAN IP address.
InterJet GUI	On the InterJet's LCD, these values are displayed and can be set on the Network Settings screen (main menu #3, option #2). The network address and netmask can be examined and set by editing the Perimeter Ethernet network entry from the System Agent's Network View page. Then, the InterJet's IP address on that network can be set by editing the InterJet's machine entry.

Table 3-1 Account Fields (continued)

Enable DHCP Dynamic Range	
Description	Enable DHCP on this net Select the check box to enable DHCP for the Perimeter network. When enabled, the DHCP server responds to requests from DHCP clients (such as Windows 95 and Macintosh systems) by dynamically assigning IP addresses, rather than requiring that static IP addresses be assigned. This is the preferred method. DHCP dynamic range Sets the range available for DHCP allocation relative to the network address. A customer might want some number of static addresses available for non-DHCP-capable devices. The default is to use the top half of the available network addresses for dynamic assignment to DHCP clients.
InterJet GUI	These and other DHCP values can be set by editing the Perimeter Ethernet network entry in the System Agent's Network View page. The Perimeter network DHCP settings are not displayed on the InterJet's LCD.
Section: Internet Connection	
When to Connect	
Description	Dial-on-demand If you select this option, set the number of minutes for idle timeout. This option applies only to InterJets using POTS or ISDN to make the Internet connection. Since most customers must pay for the use of telephone lines, dial-on-demand is preferred for these connection types. This setting is ignored if the InterJet connects via a synchronous serial line or local gateway. Full-time connection Select this option for InterJets that use the synchronous serial or leased line connection, or if the InterJet is to stay permanently connected over POTS or ISDN.

Table 3-1 Account Fields (continued)

InterJet GUI	WhistleWare 1.x: This field value is displayed and editable on the System Agent's Network Ports details pages for the modem and ISDN ports. WhistleWare 2.x: This field value is displayed and editable on the System Agent's Connection page.
Connect to the Internet Via	
Description	Use the radio buttons to select which interface the InterJet should use to connect to your POP (Point of Presence). Select Local Gateway to reach the Internet through a local gateway on the Office or Perimeter LAN. If this option is selected, no WAN connection will be made. Select POTS to connect over an analog line using a v.34 modem. Select ISDN to connect using an ISDN BRI. Select Synchronous to connect using a synchronous protocol such as Frame Relay. Auto-configuration will fail if this is selected and the InterJet does not have the internal synchronous serial card.
InterJet GUI	The System Agent's Network General page has radio buttons that specify the use of the currently enabled WAN port or local gateway for traffic heading off the network. WhistleWare 1.x: Individual WAN interfaces can be enabled or disabled on each port's System Agent details page. WhistleWare 2.x: Individual WAN interfaces can be enabled or disabled on the System Agent's Network Ports page.
Local gateway: IP address	
Description	If you select Local Gateway, specify the IP address of a local gateway on the Office or Perimeter LAN. This must be a machine capable of routing IP traffic to the Internet.

Table 3-1 Account Fields (continued)

POTS (analog modem) Parameters: POTS# to dial Login Password Request IP Address	
Description	The PPP settings are login information for the customer's connectivity to the ISP POP (Point of Presence). Specify the InterJet WAN IP address, as needed. The default value, 0.0.0.0, indicates that the WAN IP address should be negotiated when the InterJet connects to the PPP server. If your dial-up server requires the InterJet to request a specific address, specify the address here. Note: Whistle recommends that the request IP address be the same as the InterJet's address on the Perimeter network, if the Perimeter network is configured.
InterJet GUI	These field values are displayed and editable in the Modem Port Details page when the user selects and edits the modem port from the System Agent's Network Ports page.

Table 3-1 Account Fields (continued)

ISDN (BRI) Parameters: ISDN# to dial Login Password Request IP Address	
Description	The PPP settings are login information for the customer's connectivity to the ISP POP (Point of Presence). Specify the InterJet WAN IP address, as needed. The default value, 0.0.0.0, indicates that the WAN IP address should be negotiated when the InterJet connects to the PPP server. The number to dial must be that of an NAS capable of receiving an incoming ISDN BRI call. If your dial-up server requires the InterJet to request a specific address, specify the address here. Note: Whistle recommends that the request IP address be the same as the InterJet's address on the Perimeter network, if the Perimeter network is configured.
InterJet GUI	When the user selects and edits an ISDN/external serial port from the System Agent's Network Ports page, these field values are displayed and editable on the Port Details page.
ISDN (BRI) Parameters: Switch Type Line 1 Phone # Line 2 Phone # Line 1 SPID Line 2 SPID Options	
Description	Set the telephone and SPID numbers for the 2 channels, and set the ISDN switch type. You can select any of the options for channel bonding (if you specify two channels), 56 KB/64 KB channels, and CHAP authentication. Select Use voice mode if the ISDN BRI is set up for voice only (not data). Note: European switch types do not require SPIDs, directory numbers, or CHAP authentication, so these fields can be left blank.

Table 3-1 Account Fields (continued)

InterJet GUI	When the user selects and edits an ISDN/external serial port from the System Agent's Network Ports page, these field values are displayed and editable on the Port Details page.
Synchronous (external CSU/DSU) Parameters:	
InterJet GUI	For InterJets that have a synchronous port, these field values are displayed and editable in the Synchronous Port Details page when the user selects and edits the synchronous port from the System Agent's Network Ports page.
Protocol	
Description	Use the radio buttons to select the synchronous protocol to be used: Raw Synchronous, Cisco HDLC, or Frame Relay. Your selection depends on the protocol supported by your back-end synchronous equipment. If you select Frame Relay, enter a single DLCI to be used for the connection. The InterJet automatically determines the appropriate LMI.
Local IP Remote IP	
Description	Enter the IP addresses to be used for the synchronous connection. The InterJet's local IP address must be routable from the Internet. It is used as the source address for all outgoing traffic from the InterJet itself and from LAN client machines (when address translation is enabled). If PPP mode is enabled, these addresses are used in IPCP negotiation. Note: Whistle recommends that the local IP address be the same as the InterJet's address on the Perimeter network, if the Perimeter network is configured.

Table 3-1 Account Fields (continued)

Options	
Description	Select a type of encapsulation to be used over the Frame Relay or Raw Synchronous connection. rfc 1490 This type of encapsulation is generally used with the Frame Relay protocol. It does not apply to the Raw Synchronous or Cisco HDLC protocols. PPP mode PPP encapsulation can be used over a Raw Synchronous connection and can be used alone over a Frame Relay connection or over rfc 1490. It does not apply to Cisco HDLC. If you select PPP mode and authentication is required, enter the PPP Login and Password. Otherwise, leave these fields blank.
Section: Mail Processing	
InterJet GUI	These field values are displayed and editable in the External Mail section of the Mail Agent's Options page.

Table 3-1 Account Fields (continued)

Interval	
Description	Specify how often the InterJet will send outgoing mail and check for incoming mail. The InterJet will check the external mail servers (MX backups) for incoming mail every time the link comes up or the interval expires, whichever comes first. (The method used to trigger incoming mail delivery is specified by the mail-check method.) WhistleWare 1.x: There is a single setting for processing the mail queue that controls both internal and outgoing mail. This setting is not configured by Whistle Commander but only by the local administrator. The user sets a shorter interval to speed delivery of outgoing mail, and sets a longer interval for dial-on-demand systems to reduce frequent dialing. WhistleWare 2.x: All outgoing mail is batched and sent whenever the WAN link comes up or the interval time has expired, whichever comes first. Keep in mind that InterJet will always accept incoming mail sent directly to the InterJet whenever it is connected. The InterJet needs to check the external mail servers only after being disconnected, because any mail sent to InterJet's domain will have been queued on the ISP's mail server(s).

Table 3-1 Account Fields (continued)

Method	
Description	The InterJet provides a selection of methods to check for queued mail at the ISP. The method setting performs an action when the link comes up. The method you choose depends on how you operate your mail queues. ETRN The InterJet sends an SMTP ETRN command to the remote mail server, causing it to de-queue any mail for the InterJet's domain. ETRN is supported by mail servers running Sendmail 8.8 and later. (See RFC1985.) stay connected If selected, specify the minimum number of minutes the InterJet should stay online to receive mail from an ISP server. For example, if your mail server attempts to deliver mail from its queue every 15 minutes, you might have the InterJet stay online for 20 minutes at a time to guarantee that it is available for delivery. Use this method if your server does not support ETRN. finger account If selected, the InterJet fingers the specified account to trigger a queue run for the domain. Requires a modified finger daemon running on the server to trigger mail queue processing. This can achieve the same results as ETRN, but is non-standard and thus less recommended. fetch mail from POP/IMAP mailbox If this option is selected, the InterJet will get mail from the specified POP or IMAP mailbox on the ISP's server. Specify the password required to access the indicated mailbox. This option requires you to set up the mail server and MX records such that all mail for the InterJet's domain gets delivered to the specified mailbox for the InterJet to pick up in this fashion. This option is available only in WhistleWare 2.x; auto-configuration will fail if this option is selected and the InterJet is running WhistleWare 1.x.

Table 3-1 Account Fields (continued)

Section: Web Mirroring	
InterJet GUI	WhistleWare 2.x: These field values are displayed and editable on the Webmaster Agent's Setup page. WhistleWare 1.x: These field values are displayed and editable on the Webmaster Agent's Options page.
Mirror to	
Description	Specify the fully qualified domain name (or IP address) of the computer to which the InterJet should copy its public Web site via FTP. Whistle recommends using your name for the server (something like <code>webfarm1.isp.net</code>). If you are using <code>www.<InterJet_domain>.com</code>, the www resolves to field must specify an IP address for the external Web host, or the InterJet will not be able to resolve the name. If this field is left blank, mirroring information will not be configured on the InterJet.
Login Password Path	
Description	Specify the login name and password the InterJet should use when using FTP to send Web pages to the server specified in the Mirror to field. You can also specify a path (relative to the login's home directory) if the Web pages should be mirrored to some location other than the login's home directory.
Section: Server Names	
InterJet GUI	The names/machine mappings for <code>www</code> and <code>ftp</code> can be viewed and set by editing the appropriate machine entries on the System Agent's Network View page.

Table 3-1 Account Fields (continued)

'www' resolves to	
Description	Use the radio buttons to specify which computer (if any) the name <code>www.<InterJet_domain>.com</code> should resolve to, so that LAN and Internet clients can find the organization's public Web pages by that name. The InterJet creates a DNS entry with this name for the machine you specify. Note: Your name server should also have a DNS entry for this name, unless your name server is secondary to the InterJet's domain (that is, the InterJet is connected full-time and your server gets zone transfers from it). Nothing No DNS mapping is created on the InterJet for the name <code>www</code>. InterJet's external IP address Select this option if the customer's public Web site will be hosted on the InterJet itself. (WhistleWare 1.x does not support this feature. Auto-configuration will fail if this option is selected and the InterJet is running WhistleWare 1.x.) External Web Host Select this option if the customer's public Web site will be hosted on a computer other than the InterJet (on your backbone, for example, or on the InterJet's Perimeter network). If this option is selected, you must specify the name (or IP address) of the external Web host. If mirroring is configured, this will generally be the same as the Mirror to server. For a public Web server on the Perimeter network, you must specify the server by its IP address on the Perimeter network.

Table 3-1 Account Fields (continued)

'ftp' resolves to	
Description	Use the radio buttons to specify which computer (if any) the name ftp.<InterJet-domain>.com should resolve to, so that LAN and Internet clients can find the organization's public FTP server by that name. The InterJet will create a DNS entry with this name for the machine you specify. Nothing No DNS mapping is created on the InterJet for the name ftp. InterJet's external IP address Select this option if the customer's public FTP site will be hosted on the InterJet itself. (WhistleWare 1.x does not support this feature. Auto-configuration will fail if this is selected and the InterJet is running WhistleWare 1.x.) External FTP Host Select this option if the customer's public FTP site will be hosted on a computer other than the InterJet (on your backbone, for example, or on the InterJet's Perimeter network). If this option is selected, you must specify the name (or IP address) of the external FTP host. For a public FTP server on the Perimeter network, you must specify the server by its IP address on the Perimeter network. Note: If the FTP server is not the same as the Web server, any external FTP server will need to be maintained and administered manually.
Section: Time	
InterJet GUI	These field values are displayed and editable in the Time Setting section of the System Agent's Network General page.

Table 3-1 Account Fields (continued)

NTP Server Alternate	
Description	Specify the NTP (Network Time Protocol) servers the InterJet should poll to keep its clock synchronized. Whistle recommends that these fields specify NTP servers on your backbone, but if you have none, there are many public servers available on the Internet. Information about NTP and using public servers can be found at http://www.eecis.udel.edu/~ntp. If this option is not configured, the InterJet clock can drift over time. Because the InterJet is also an NTP server on the LAN, this can affect any clients that synchronize their clocks from the InterJet.
Time Zone	
Description	NTP specifies the current time in Greenwich Mean Time. The InterJet uses the time zone to translate to local time and compensate for local observance of Daylight Savings Time, if applicable. Select a city in the same time zone as the InterJet. Select <i>unspecified</i> if you do not know or do not want to configure the InterJet's time zone.
Section: Service Provider Info	
InterJet GUI	These fields are displayed in the ISP Agent's Information page. They are not editable by the local administrator.
ISP Name	
Description	Enter your ISP name.
Acct Info URL	
Description	Specify a URL from which the local administrator can get information about their account with you. It should be in the form: <code>http://server.isp.net/services</code>

Table 3-1 Account Fields (continued)

Support URL	
Description	Specify a URL from which the local administrator can get information about your technical support services. It should be in the form: <code>http://server.isp.net/support.</code>
Upgrade Server Upgrade Path	
Description	The InterJet is capable of downloading new system software on the Internet, either directly from Whistle or from the server and path that you specify. Whistle recommends that you have copies of Whistle's latest software releases available for your InterJet customers to download. If you choose to make software upgrades available from your site, specify the upgrade server as something like <code>ftp.isp.net</code>. This server must have anonymous FTP enabled to facilitate downloading of new systems. The path indicates which directory on the server contains the upgrade images. To allow software upgrades directly from Whistle, specify the server as <code>ftp.whistle.com</code> and the path as <code>/interjet</code>.

Lockdown Fields

When you select the check box labeled **Lockdown** in the **Auto-Configuration Status** section, a specific set of fields in the InterJet's administrative pages are locked. When fields are locked, they are not locally editable. All lockable fields are either locked or unlocked; fields cannot be locked individually. The set of lockable fields is predetermined.

Table 3-2 shows the fields that are locked when lockdown is enabled, and also shows some related fields that are never locked.

Table 3-2 Lockable and Non-lockable Fields

Lockable Fields	Non-lockable Fields
DNS information, including the InterJet's domain, forwarders, and MX backups	
Host address translation ON or OFF	
NTP servers	
LAN-side IP address and netmask	LAN DHCP settings are not locked. InterJet names on the LAN are not locked.
Perimeter IP addresses Perimeter network enablement/disablement	Perimeter DHCP settings are not locked. InterJet names on the Perimeter network are not locked.
Port used to access the Internet (POTS, ISDN, synchronous, or local gateway)	
POTS configuration: phone number, PPP login and password, and request IP	
ISDN configuration: phone number, PPP login and password, request IP, switch type, line numbers, SPIDs, and options	
External serial port configuration	
Synchronous port configuration: protocol, IP addresses, RFC 1490, PPP mode, login, and password	

Table 3-2 Lockable and Non-lockable Fields (continued)

Lockable Fields	Non-lockable Fields
Mail-check method	The local administrator can adjust the mail-check interval.
Full-time connection or dial-on-demand setting	Dial-on-demand timeout; that is, if dial-on-demand is locked down, the local administrator can still control timeout. Blackout periods are not controlled by Commander.
Secondary name servers	

Setting Up Default Values

Most of the editable fields in the account edit page are automatically filled in with default values. The default values for these fields are specified in the `defaults` file:

```
${HTTPBASEDIR}/whistle/interjet/admin/Databases/  
defaults
```

You can edit this file with any text editor to modify the default values for your site. The variables in the file correspond directly to the editable fields in the New/Edit Account page. The values that you specify are shown as the default values for any new account that you create after editing the file. Existing accounts are not affected by changes that you make to the `defaults` file.

A sample `defaults` file is provided below. This sample shows the default settings that are downloaded with the system. You must customize the following values, either in the `defaults` file or for each account:

- DNS forwarder IP addresses
- PPP account info `ppptelno` (the other fields are specific to each account)
- Time configuration `ntpserver` addresses
- Web Mirroring `mirrornetaddr` and `mirrorname`
- ISP information `ispname`, `ispaccturl`, and `ispsuppturl`

Sample Configuration Files

Sample Globals File

```
# global settings for this Commander
# ip address for IJ's to get configuration from.
# IJ will make http request using URL:
# "<acipaddr>/whistle/interjet/autoconfig.cgi?regid=xxxxxxx"
# if this is left blank, recv-acct-edit.cgi will attempt to
# determine commander's ip address using 'hostname' system
# command and 'gethostbyname' function, which may not
# correctly determine the web server's address on
# multi-homed systems...
acipaddr = 207.76.205.100
# phone number to dial for auto-configuration
# NOTE: this is only displayed on summary setup page
acphone = 1-800-555-1234
```

Sample Defaults File

```
# default settings to use for new accounts...
# default auto-conf mode: disabled, only, any
acmode = only
# lockdown: on, off
# if on, disallows IJ's local admin from modifying
# certain configuration fields
lockdown = off
# DNS info
domain = orgname.com
# forwarding nameserver(s). (ip address)
forwarder1 =
forwarder2 =
# machine(s) accepting/holding mail for IJ when
# not connected (FQDN)
mxbackup1 = mail-host1.isp-domain
mxbackup2 =
# Microsoft filessharing (SMB) workgroup name
# if blank, commander will not set IJ's workgroup name,
```

```
# although IJ's Network Neighborhood filessharing will
# still be enabled.

workgroup = WORKGROUP

# (Note: "WORKGROUP" is the default workgroup for
# stock Win95 machines...)

# InterJet's address on Office LAN and number of bits in
# network mask, for example, 192.168.1.1/24 (if no / is
# found, assumes /24)
# (ip address may be omitted to only default netmask, eg: /28)
ijlanaddr = 192.168.1.1/24

# IMPORTANT! if address translation is NOT enabled
# (this is not recommended), the addresses assigned to the
# Office LAN MUST be routable, or the outside world will
# not be able to respond to clients.
# address translation: on, off.
# Whistle strongly recommends enabling this for all accounts!

nat = on

# active ftp: on, off.
# if on, IJ's firewall will allow active ftp from Office
# LAN - not recommended

activeftp = off

# Office LAN DHCP server on, off

dhcp = on

# dhcp dynamic range expressed as offsets from network
# address. NOTE: make sure that range fits on network
# specified by netmask, above!

dhcpstart = 128
dhcpend = 254

# for example, if net address is 192.168.1.32 and range
# is 16-30, then # 192.168.1.48 through 192.168.1.62 are
# available for dynamic addressing.

# InterJet's address on Perimeter and number of bits in
# network mask: for example, 207.76.204.0/24 (if no / is found,
# assumes /24)
# (ip address may be omitted to only default netmask,
# eg: /28)

ijperaddr = /28

# IMPORTANT! addresses assigned to perimeter net MUST be
# routable, as they are intended to be reached from the
```

```
# outside world...
# Perimeter LAN DHCP server on, off
perdhcp = off

# dhcp dynamic range expressed as offsets from
# network address. NOTE: make sure that range fits on network
# specified by netmask, above!

perdhcpstart = 8
perdhcpend = 14

# for example, if perimeter address is 207.76.204.1 and
# range is 8-14, then # 207.76.204.8 through 207.76.204.14 are
# available for dynamic addressing.

# POTS PPP account info
ppptelno = 555-1234
ppplogin = OrgName-IJ
ppppassword = random
ppplocaladdr = 0.0.0.0

### isdn configuration stuff
# ISDN PPP account info

isdntelno = 1-415-555-1234
isdnlogin = OrgName-IJ
isdnpasswd = random
isdnlocaladdr = 0.0.0.0

# central office switch type:
# ni1, dms100, 5ess-p2p, 5ess-mp, net3, 1tr6, vn3,
# ins64, sing, aus
coswitch = net3

# isdn options: on, off
chap = on
bear56k = off
bonding = on

# no defaults for directory numbers or spids...
spid1 =
spid2 =
dirno1 =
dirno2 =

# Sync port configuration
syncprotocol = frame-relay
# protocol: frame-relay, cisco-hdlc, raw-sync
syncdlci = 16
```

```
# dlci, applies only to frame-relay
sync1490 = on
# on/off, applies only to frame-relay
syncppp = off
# on/off, may apply to frame-relay or raw-sync
synclocaladdr =
# IJ's ip address on sync connection
syncremoteaddr =
# remote device's IP address on sync connection
synclogin =
# only used if PPP enabled and requires auth
syncpassword =
# only used if PPP enabled and requires auth
# dial-on-demand timeout. Set to zero for Full-Time
# connection.
dodtimeout = 10
# dodtimeout = 0
# mail configuration parameters
# how often to send outgoing & check for incoming mail,
# in minutes
mailinterval = 30
# method to use to check for incoming mail:
# donothing, stayconnected, fingeracct, fetchmail
togetmail = donothing
# minimum connection time, if method is stayconnected
minconnect = 15
# account to finger, if method is fingeracct
accttofinger = orgname@mail-host1.isp-domain
# POP/IMAP account to fetch from, if method is fetchmail,
# and password to use
fetchfrom = orgname@mail-host.isp-domain
fetchpasswd = random
### time configuration
# name or ip addresses of closest Network Time Protocol
# server(s)
```

```
ntpserver1 = ntp.isp-domain
ntpserver2 =

# timezone is a pathname relative to /usr/local/zoneinfo on
# a BSD Unix machine
# eg: America/Los_angeles, Europe/Amsterdam, Pacific/Tahiti
# may be left blank (or set to 'unspecified') to NOT configure
# interjet's timezone.

timezone =      America/Los_Angeles

### Web Mirroring
# specify server's name and login info to configure InterJet
# for mirroring
# leave mirrorname blank to NOT configure mirroring

mirrorname = webhost.isp-domain
mirrorlogin = OrgName
mirrorpassword = random
mirrorpath = .

### Server names
# specify which machine (if any) is www.local-domain and/or
# ftp.local-domain
# www maps to: nothing, interjet, ext_host

wwwis = ext_host

# if (wwwis = ext-host), specify the external host by FQDN
# (eg: webhost.isp-domain), or by IP address (on your backbone)
# or IJ's Perimeter LAN)

ext_web_host = webhost.isp-domain

# Note: generally, if mirroring is configured above, you will
# want the name www to map to the mirror, so set wwwis to
# 'ext-host' and ext-web-host to the mirrorname

# ftp maps to: nothing, interjet, ext-host
# same concept as for wwwis, above, but maps the name
# 'ftp.local-domain'

ftpis = nothing
ext_ftp_host =

# ISP info here...

ispname = Your ISP Name Here
ispaccturl = http://www.isp-domain/account-info.html
ispsupturl = http://www.isp-domain/tech-support.html

# Where can IJ get WhistleWare upgrades (via anonymous ftp)

upgradeserver = ftp.isp-domain.com
upgradepath = interjet/upgrades/
```

```
# which interface to use for WAN connection
# 'internal', 'external', 'sync' or 'local'
useport = internal

# Note: use 'internal' for POTS and 'external' for ISDN
# (whether ij has internal card or using external async port)
# (for historicalreasons...)

# defaults for org info fields, where appropriate/useful
orgname =
orgcontact =
orgemail =
orgphone =
orgfax =
orgaddress =
orgaddress2 =
orgcity =
orgstate = CA
orgzip =
orgcountry = US
```




Whistle Communications Corp.
110 Marsh Drive
Foster City, CA 94404
U.S.A.