



NET INTEGRATION TECHNOLOGIES INC.



NET INTEGRATOR User Manual

Version 3.74

This device complies with IEC60950 (1999) 3rd Edition, CSA C22.2 No. 60950-00/UL 60950 (2000) 3rd Edition.

Federal Communications Commission (FCC) Compliance Information Statement

This equipment has been tested and found to comply with the limits for either Class A or Class B digital devices (refer to “Requirements Compliance”), pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Requirements Compliance

The Net Integrator Lite, Mark I, and Mark II systems meet Class B requirements. The Net Integrator Mark IIIR meets Class A requirements.

Operating Conditions

Net Integrator Lite, Mark I, and Mark II:

- 100V – 127VAC 60Hz / 10A
- 200V – 240VAC 50Hz / 5A
- 0 to 35 degrees Celsius
- 5% – 90% Relative Humidity

Net Integrator Mark IIIR:

- 100V – 240VAC / 8A – 4A
- 50Hz - 60Hz
- 0 to 35 degrees Celsius
- 5% – 90% Relative Humidity

Changes or modifications not expressly approved by Net Integration Technologies Inc. could void the user's authority to operate the equipment.

Publication Date: November 2003

Chapter 1

First-time Setup 11

- Net Integrator Technical Support 11
- Net Integrator Components 11
- Meet Your Net Integrator 12
- Connecting the Power 15
- Ethernet Connections 16
- Connecting Ethernet Port 0 17
- Connecting Ethernet Ports 1 and 2 18
- Connecting an External Dial-up Modem 19
- Power-up Sequence 20
- Manually Setting the IP Address 21

Chapter 2

Connecting to WebConfig 23

- What is WebConfig? 23
- Secure WebConfig 23
- Configuring TCP/IP 24
- Creating an Administrator Account 35
- System Status Screen 40

Chapter 3

Configuring your Net Integrator 45

- Proceeding with Configuration 45
- Configuring General Network Settings 45
- Configuring Advanced Network Settings 47
- Network Devices 48
- Network Routes 50
- Network Configuration Scenarios 52
- Configuring your Internet Connection 55

<i>Chapter 4</i>	<i>DoubleVision</i> 59
	What is DoubleVision? 59
	Modem Connections 60
 <i>Chapter 5</i>	 <i>User & Team Management</i> 61
	Service Integration 61
	User Accounts 62
	Modifying User Email Settings 69
	Team Accounts 71
 <i>Chapter 6</i>	 <i>File Services</i> 77
	File Sharing Services 77
	Configuring File Services 77
 <i>Chapter 7</i>	 <i>Domain Controller</i> 79
	What is a Domain Controller? 79
	Configuring the Domain Controller 79
	Joining Windows Systems to a Domain 80
	File Mounting/Drive Mapping 87
	Logon Scripts 88
	Automated Drive Mapping 89
 <i>Chapter 8</i>	 <i>Print Services</i> 91
	Net Integrator Print Services 91
	Configuring Print Services 91
	Configuring your Workstation 92

Chapter 9

Email Services 95

Components of the Email System	95
Configuring Email Service	96
Clearing the Email Queue	98
Configuring Email Aliases	99
Configuring DNS Records	103
Configuring Email Clients	104
Advanced Email Settings	106
LDAP Server	107

Chapter 10

WebMail 111

WebMail Server	111
Enabling WebMail Server	111
Accessing WebMail	113
Configuring WebMail	116
Composing an Email Message	117
Opening a Received Message	118
Replying to a Message	119
Search Function	119
Address Book	120
Calendar	122
Tasks	123
Memos	124
Mail Filters	125

Chapter 11

Web Services 129

Web Server	129
Master Web Server	129
Virtual Web Servers	133
Hosting Multiple Web Sites	135

Secure Web Services **136**
SSL Certificate **136**
Web Caching **141**

Chapter 12

Web Filtering 143

Positive Web Filtering **143**
Enabling the Web Filter **143**
Providing Full Internet Access **144**
Adding Permitted Websites **145**
Accepting Access Requests **145**
Denying Access Requests **146**
Entering Access Requests **147**

Chapter 13

FTP Services 149

FTP Server **149**
Anonymous FTP Server **149**
Enabling the FTP Server **150**
Enabling FTP Access **151**
User vs. Team FTP Access **151**

Chapter 14

Backup & Restore 153

Intelligent Disk Backup (idb) **153**
Configuring idb **154**
Initiating an idb Backup **155**
idb Restore **158**
Initiating an idb Restore **158**
idb Backup Teams **162**
idb Hot Swap **162**
Swapping idb Hard Disks (with Hot Swap) **164**

Swapping idb Hard Disks (without Hot Swap) **167**

Tape Backup **170**

Initiating a Tape Backup **170**

Tape Restore **174**

Initiating a Tape Restore **175**

Chapter 15

Software Update 177

Software Updates **177**

Upgrading your Net Integrator **177**

Chapter 16

TunnelVision 181

Private Networks **181**

Virtual Private Networks **181**

How TunnelVision Works **183**

Creating a VPN (server-to-server) **184**

Configuring a TunnelVision Master Server **185**

Configuring a TunnelVision Client **186**

TunnelVision Status **187**

The Idle Time-out **187**

Chapter 17

IPsec 189

IPsec: An alternative to TunnelVision **189**

Known Configurations **189**

Adding an IPsec route **190**

Adding an Anonymous Incoming Connection

IPsec route **191**

Editing an IPsec route **192**

Setting up Third Party IPsec Clients **194**

<i>Chapter 18</i>	<i>Remote Access Services</i>	197
	What is RAS?	197
	PPTP - Client-to-Server VPN Service	197
	Dial-in Service	203
	Terminating a Connection from WebConfig	207
 <i>Chapter 19</i>	 <i>Firewall Services</i>	 209
	ICSA Firewall Security Compliance	209
	Traffic Denied Inbound	209
	Traffic Permitted Inbound	210
	Traffic Permitted Outbound	210
	Firewall Log	211
 <i>Chapter 20</i>	 <i>Domain Name Services</i>	 213
	What is DNS?	213
	DNS Services	213
	Configuring Public DNS	214
	How the DNS System Works	215
	Dynamic DNS	216
	Manually Creating DNS Entries	216
 <i>Chapter 21</i>	 <i>Workstation Viewer</i>	 221
	What is the Workstation Viewer?	221
	Accessing the Workstation Viewer	221
	Virtual Network Computing (VNC)	222
	Configuring VNC	222

Chapter 22

FastForward 225

- What is FastForward? 225
- Introduction to TCP/IP 225
- Proxy Servers 227
- Configuring FastForward 229
- Forwarding Scenarios 231
- Multiple Static IP Addresses 232
- Common Port Numbers 232
- Troubleshooting FastForward 233

Chapter 23

Disk Management 235

- Disk Configuration (idb and RAID) 235
- Reconfiguring your disks 236
- Disk Status Messages 238
- Recovering from Disk Failure 239
- Disk Recovery (SystemER) 241
- Hard Disk Failure 241
- Installing a New Hard Drive 242

Chapter 24

MySQL Server 247

- What is the MySQL Server? 247
- What is phpMyAdmin? 247
- Managing Databases in phpMyAdmin 248
- Setting up Windows for MySQL Access 252
- What is a Dynamic Web Site? 256

Chapter 25

Log Messages 257

- Accessing Log Messages 257
- Customizing Message Display 258

Firewall Log 258

Chapter 26 *Network File System* **261**

What is NFS? 261

Installing and Configuring `ugidd` 261

Mounting an NFS directory 262

Unmounting an NFS Directory 262

Chapter 27 *rsync* **263**

What is `rsync`? 263

Using `rsync` 263

GNU General Public License 265

Licensing 271

GNU Lesser General Public License 273

The “Artistic License” 283

Zlib License 287

Apache Public License 289

The PHP License, version 2.02 291

BSD License 293

Glossary 295

ExchangeIt! Addendum 313

Net Integrator Technical Support

If you need technical support, please contact your Net Integrator reseller.

Authorized Resellers may contact the toll-free Reseller Technical Support Line:

1-86-NET-ITECH (1-866-384-8324)

Outside of North America call **905-946-1777**

Hours of operation: 8:30 am to 5:30 pm EST, Monday to Friday

Net Integrator Components

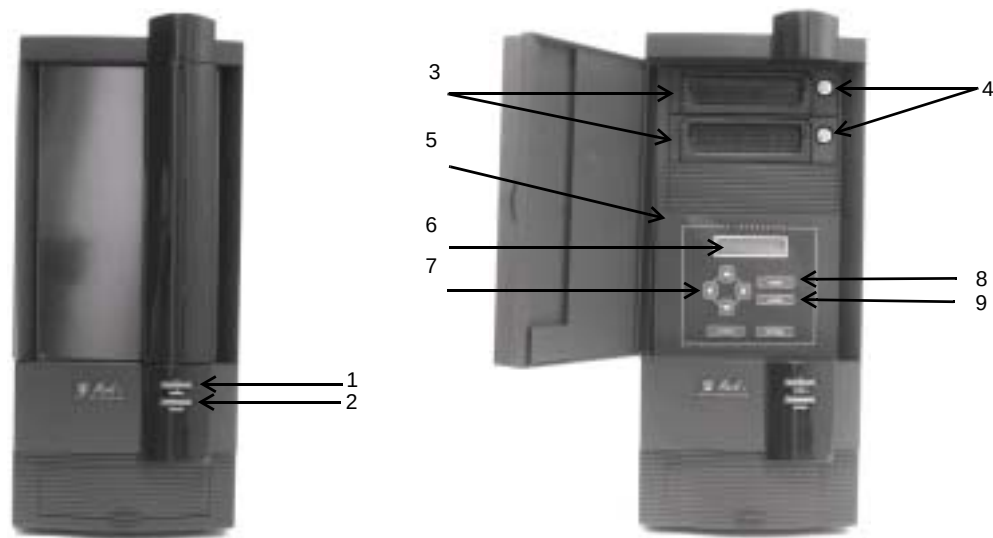
You should have received the following components in your Net Integrator package:

1. Net Integrator Server (1)
2. Net Integrator User Manual and Quick Start Guide CD (1)
3. Hard disk keys (2) - Lite/Mark I/ Mark II or Face Plate Keys (2) - Mark IIIR
4. Power supply cord (1)
5. Category 5 Ethernet cables (3)

Meet Your Net Integrator

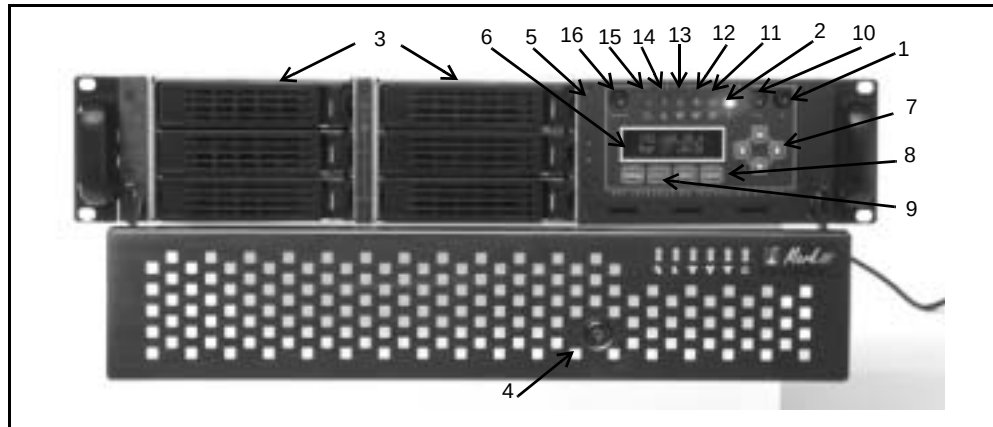
Front View

The following image is of a Net Integrator idb model. Net Integrator 'tape' models are similar to idb models but are equipped with a tape backup drive instead of an Intelligent Disk Backup (idb) system.



Please Note: This image corresponds to our Lite, Mark I and Mark II models.

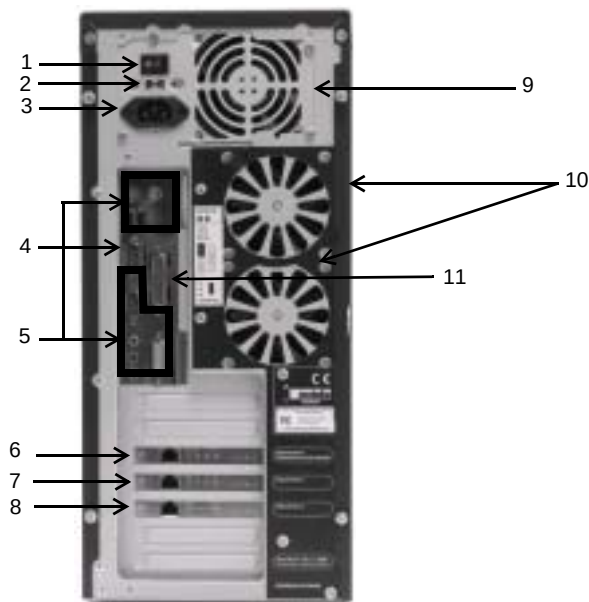
1. **Power button** – used to turn the box on and off.
2. **Internet Status light** – lights up when you are connected to the Internet.
3. **Removable hard disk trays** – houses the hard disk(s).
4. **Hard disk key lock** – locks the face plate preventing physical access.
5. **Control panel** – contains the display panel and all control buttons.
6. **Display panel** – displays the status of the Net Integrator.
7. **Direction arrows** – used to execute commands from the control panel.
8. **Enter and Cancel buttons** – used to execute commands from the control panel.
9. **Backup and Restore buttons** – used to initiate backup and restore procedures.



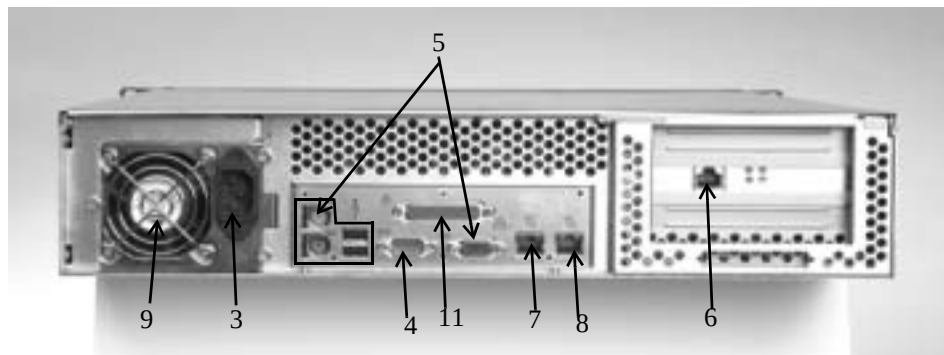
Please Note: The image above corresponds to our Mark III R model.

1. **Power button** – used to turn the box on and off.
2. **Power LED** – lights up when unit is powered.
3. **Removable SCSI drive trays** – houses the hard disk(s).
4. **Face plate key lock** – locks the face plate preventing physical access.
5. **Control panel** – contains the display panel and all control buttons.
6. **Display panel** – displays the status of the Net Integrator.
7. **Direction arrows** – used to execute commands from the control panel.
8. **Enter and Cancel buttons** – used to execute commands from the control panel.
9. **Backup and Restore buttons** – used to initiate backup and restore procedures.
10. **Reset Button** - used to reset the system (normally disabled).
11. **Ethernet 0 Activity** - indicates activity on the Ethernet 0 interface.
12. **Ethernet 1 Activity** - indicates activity on the Ethernet 1 interface.
13. **Ethernet 2 Activity** - indicates activity on the Ethernet 2 interface.
14. **Over-temperature indicator** - lights up if the internal temperature is too high.
15. **Fan failure indicator** - lights up if the front internal fans fail.
16. **Buzzer off** - turns off audible alarm from over-temperature or fan failure.

Back View



Please Note: The image above corresponds to our Lite, Mark I and Mark II models.



Please Note: The image above corresponds to our Mark IIIIR model.

1. **Main power switch** – used to turn the box off. The main power switch must be turned on for the power button on the front panel to work. Note: This is on our Lite, Mark I and Mark II models only.
2. **AC power selector** – indicates the voltage used in your country. Note: This is on our Lite, Mark I and Mark II models only.
3. **Power socket** – where the power cord is connected.
4. **Serial port** – for an external dial-up modem.
5. **Extra ports** – reserved for future use.
6. **Ethernet Port 0** – used to connect to the local area network (LAN).
7. **Ethernet Port 1** – used to connect to a LAN segment or to the Internet.
8. **Ethernet Port 2** – used to connect to a LAN segment or to the Internet.
9. **Power supply fan** – provides cooling for internal components.
10. **Primary and secondary cooling fans** – provides additional cooling for internal components. Note: This is on our Lite, Mark I and Mark II models only.
11. **Parallel printer port** – used for a shared printer.

Connecting the Power

1. Ensure that the Net Integrator has adequate ventilation. Place the back of the unit at least one to two feet (12"-24") away from the wall. Make sure the front of the unit is easily accessible.
2. Connect one end of the power cord into the power socket on the back of the Net Integrator:



Above: Lite, Mark I, Mark II
Right: Mark IIIR



3. Connect the other end of the cord into a standard power outlet.
4. Turn on the main power switch (located above the power cord).

Ethernet Connections

What is Ethernet?

Ethernet connects computers in a local area network (LAN). An Ethernet connection is very fast, and unlike modem and ISDN connections, one Ethernet network can have many computers attached to it. There are two different kinds of Ethernet cables: category 3 and category 5 are two examples. It is recommended that you use category 5 at minimum for 100baseT networks, and category 5e at minimum for 1000baseT networks.

10baseT, 100baseT, and 1000baseT hubs and switches have a number of ports that you connect to workstations, routers, servers, printers, or other devices using Ethernet cables. Connect your Net Integrator to a free port using one of the supplied category 5 cables. If the port lights up after you connect and then turn on your Net Integrator, you have a proper connection.

You can cascade more hubs or switches to increase the number of available ports, (consult the manual that comes with your hub/switch before trying this).

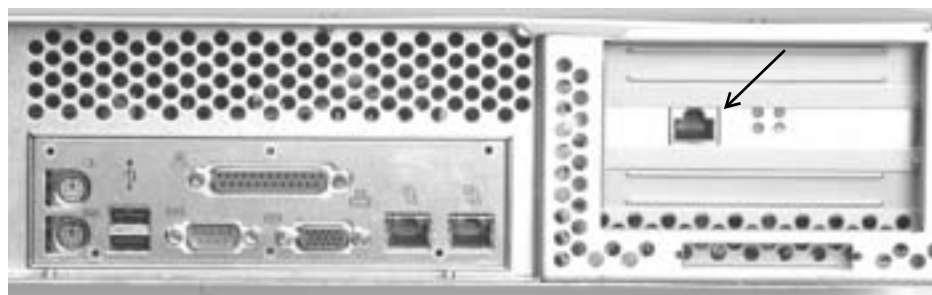
Connecting Ethernet Port 0

1. Connect one end of an Ethernet cable into *Ethernet Port 0* (located on the back of your Net Integrator).



Left: Lite, Mark I, Mark II

Below: Mark IIIR



2. Connect the other end of the cable into your LAN hub or switch.

Please Note: *Ethernet Port 0* should not be connected to a router providing Internet access. *Ethernet Port 0* is typically used/reserved for internal/Local Network access.

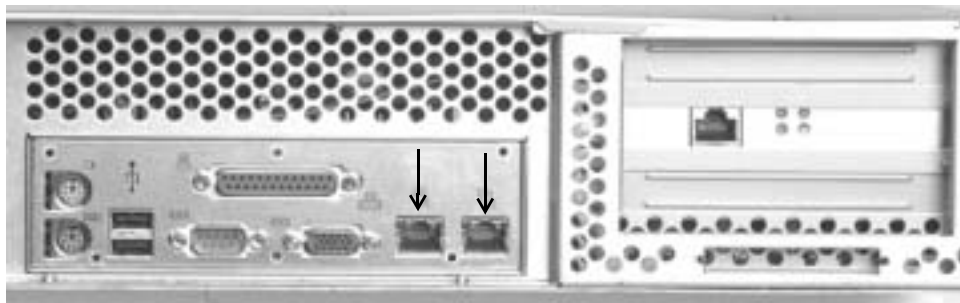
Connecting Ethernet Ports 1 and 2

Ethernet ports 1 and 2 are used to connect to the Internet or to other segments of your LAN. Use an Ethernet cable to connect to your high-speed Internet routing device. Some devices may require the use of a cross-over cable that is normally supplied with the device.



Left: Lite, Mark I, Mark II

Below: Mark IIIR



If you are using your Net Integrator as a workgroup server without a direct connection to the Internet, it is possible to use Ethernet ports 1 and 2 to connect to other segments of the LAN. This is typically done to improve network throughputs when large numbers of users are connected to Net Integrator.

Please Note: Secondary segments must be physically separate from the primary network segment connected to the ethernet 0 port. You cannot connect all ethernet ports to the same segment in order to improve network throughput.

Connecting an External Dial-up Modem

1. Connect the cable included with your own external dial-up modem to the *Serial* port on the back of your Net Integrator.



2. Connect one end of the standard telephone cable to the external modem, and connect the other end to your telephone wall jack.

Please Note: The external modem will be auto-detected when the server goes through a power-up sequence.

Power-up Sequence

1. Turn on the main power switch (for Lite, Mark I and Mark II: on the back of your Net Integrator).
2. Press the *Power* button.



Left: Lite, Mark I, Mark II

Below: Mark IIIR



3. Net Integrator needs a few moments to start up. During the start-up you will observe the following sequence of events:
 - a. The hard drive and fans start up.
 - b. Net Integrator beeps several times.
 - c. *HELLO* appears on the display panel.
 - d. Let your Net Integrator sit undisturbed while it discovers its surroundings and auto-configures its network parameters. Messages indicating what kind of network discov-

ery is being performed appear on the display panel. After approximately 10-30 seconds, the IP address that Net Integrator has chosen for itself displays. The number will look something like this: 192.168.0.1 (based on the LAN to which it's connected).

- e. When the start-up sequence is over, the display panel shows the status of various Net Integrator systems. The first line on the display panel shows Net Integrator's IP address; the second line cycles messages displaying the current date, time, and operating system version. You are ready to proceed with the setup when an IP address appears on the display panel. In the event that the Net Integrator Server is unable to detect an appropriate IP address for your LAN, you will have to manually set the IP address for the server. Refer to *Manually Setting the IP Address* for more information.

Manually Setting the IP Address

Follow these steps if your Net Integrator is unable to automatically select an IP address (the display continues to read *Choosing Address*) or if you want to change the chosen address:

1. Press the *Enter* button on control panel. The following menu displays:
MENU [Net] Info
Dialer System
2. *[Net]* is already selected. Press the *Enter* button. The following menu displays:
NETWORK [IPAddr]
Netmask DHCP
3. *[IPAddr]* is already selected. Press the *Enter* button. The current IP address (192.168.0.1, for example) displays. If Net Integrator was unable to select an IP address, 0.0.0.0 displays.
4. Use the *Left* and *Right* direction arrows to move the cursor from digit to digit. Use the *Up* and *Down* direction arrows to increase or decrease a digit's value.
5. Press the *Enter* button. The new IP address is saved.
6. Navigate to *Netmask* using the direction arrows. Press *Enter*. The default Netmask displays.
7. Use the *Left* and *Right* direction arrows to move the cursor from digit to digit. Use the *Up* and *Down* direction arrows to increase or decrease a digit's value.
8. Press the *Enter* button. The new Netmask is saved.

9. You may also turn on or off the DHCP server (which automatically assigns IP addresses to the workstations connected to your local network). Unless you have some other server providing DHCP services, it is recommended that you turn DHCP on. To do so, navigate to *DHCP* using the direction arrows. Press the *Enter* button.
10. Navigate to *On* using the direction arrows. Press *Enter*. The DHCP server is now on.
11. Press the *Cancel* button twice to return back to the standard status display.

Connecting to WebConfig

What is WebConfig?

Although some basic system configuration can be done through the front control panel, the web-based configuration system (WebConfig) is where you will set most Net Integrator options.

Secure WebConfig

Since version 3.70, Net Integrator's WebConfig uses 128-bit encryption, protecting administrator information and passwords. Most recent versions of web browsers contain built-in support for this; you may need to upgrade your browser prior to installing 3.70 or later on your Net Integrator.

Netscape 7	http://channels.netscape.com/ns/browsers/download.jsp
Netscape (older versions)	http://wp.netscape.com/download/archive.html
Microsoft Internet Explorer 6	http://www.microsoft.com/windows/ie/default.asp
Mozilla 1.0.1	http://www.mozilla.org/releases/stable.html
Opera 6.05	http://www.opera.com/download/

If you are using Microsoft Internet Explorer version 4, 5, or 5.01, but don't want to upgrade, you can download 128-bit encryption separately:

<http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp>

Failure to support 128-bit encryption will result in WebConfig being unreachable while the Net Integrator is running version 3.70 or later.

Configuring TCP/IP

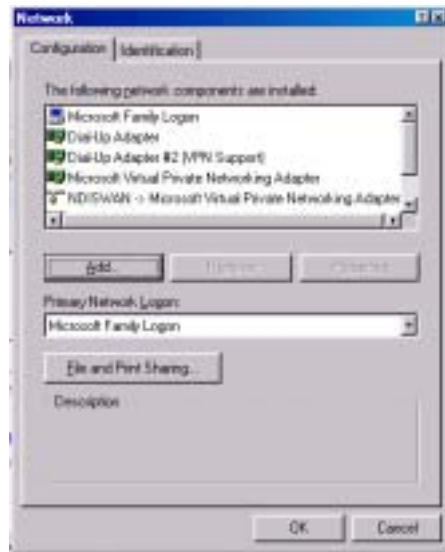
Before you can access WebConfig, you have to configure your workstation to use TCP/IP. If TCP/IP is already configured, proceed to *Creating an Administrator Account* (later in this chapter). If TCP/IP is not configured, follow the appropriate steps for your operating system.

For Windows 95/98/ME:

1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* window displays:

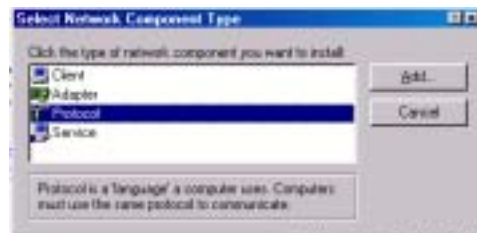


2. Select *Network* from the list. The *Network* window displays:



Click on the *Add* button if TCP/IP does not display in the installed components list.

3. The *Select Network Component* window displays:

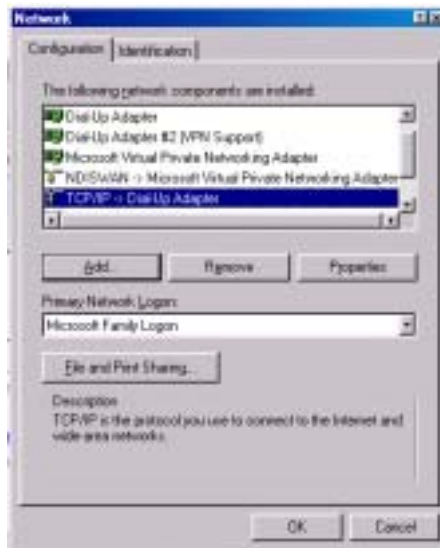


Select *Protocol* from the window. Click *Add*.

4. The *Select Network Protocol* window displays:



Select *Microsoft* in the *Manufacturers* section of the window. Select *TCP/IP* in the *Network Protocols* section of the window. Click on the *OK* button. TCP/IP should now display on the *Network* window.



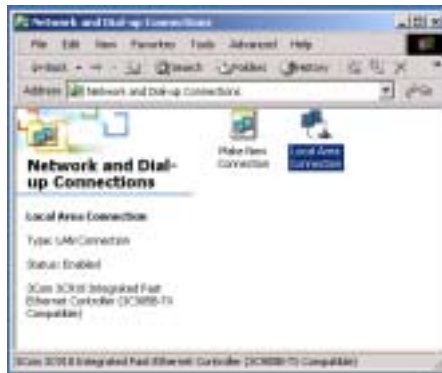
5. Select *TCP/IP* from the installed components list on the *Network* window. Click on the *Properties* button. The *TCP/IP Properties* window displays:



6. Click on the *IP Address* tab. Select *Obtain an IP address automatically*.
7. Click on the *DNS* tab. Select *Enable DNS*.
8. Select all entries in the *DNS Server Search Order* section of the window and click on the *Remove* button.
9. Select all entries in the *Domain Suffix Search Order* section of the window and click on the *Remove* button.
10. Select *Obtain an IP address automatically*.
11. Click on the *Gateway* tab. Select any entries in the *Installed gateways* section of the window and click on the *Remove* button.
12. Click on the *WINS Configuration* tab. Select all entries in the *WINS Server Search Order* section of the screen and click on the *Remove* button. Select *Use DHCP for WINS Resolution*.
13. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
14. Reboot your computer.

For Windows 2000/XP:

1. In Windows, select *Start > Settings > Control Panel* (or in Windows XP, *Start > Control Panel*).
2. Select *Network and Dial-up Connections* from the list. The *Network Connections* screen displays:

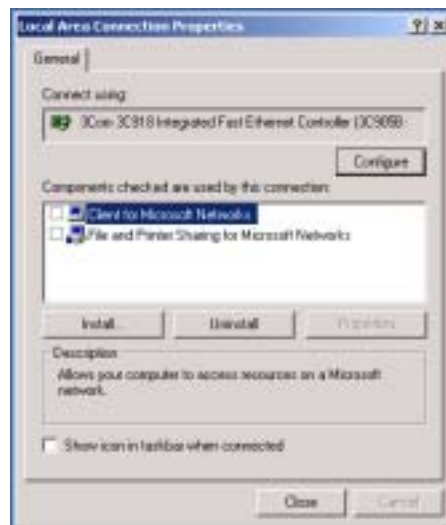


3. Click on *Local Area Connection*. The *Local Area Connection* window displays:



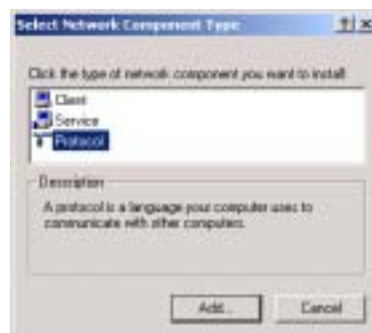
Click on *Properties*.

4. The *Local Area Connection Properties* window displays:



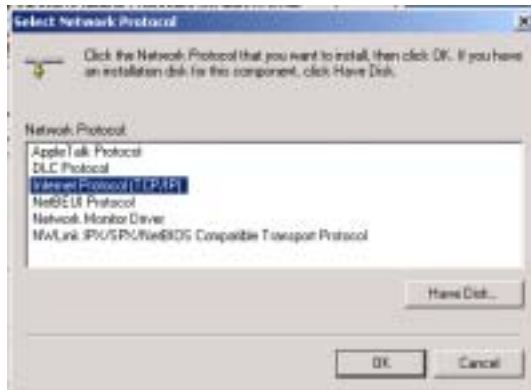
If *Internet Protocol (TCP/IP)* is not in the *This connection uses the following items* list, click on *Install*.

5. The *Select Network Component Type* displays:

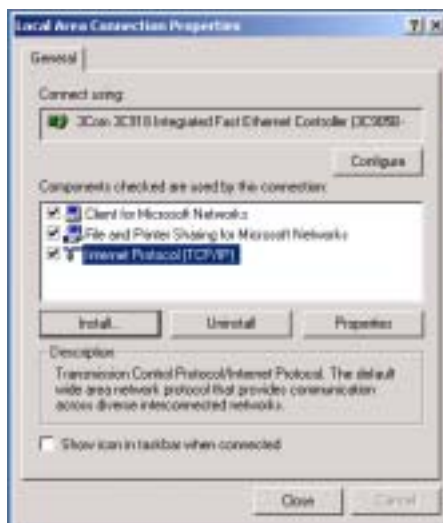


Select *Protocol* from the window. Click on *Add*.

6. The *Select Protocol* window displays:



Select *Internet Protocol (TCP/IP)* from the list. Click *OK*. TCP/IP should now display on the *Local Area Connection Properties* window.



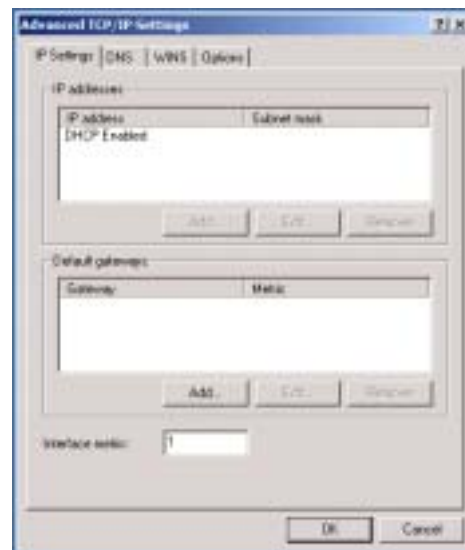
7. Select *Internet Protocol (TCP/IP)* from the list, and click on the *Properties* button.

8. The *Internet Protocol (TCP/IP) Properties* screen displays:



Select *Obtain IP Address automatically*. Select *Obtain DNS server address automatically*.

9. Click on the *Advanced* button. The *Advanced TCP/IP Settings* window displays:



Select any entries in the *Default gateways* section of the window, and click on the *Remove* button.

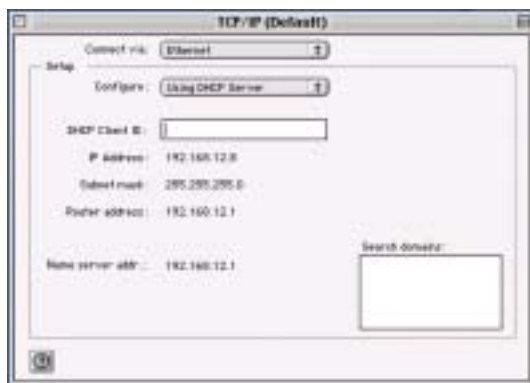
10. Click on the *DNS* tab. Select any entries in the *DNS server addresses* section of the window, and click on *Remove*. Select *Append primary and connection specific DNS suffixes*. Select *Append parent suffixes and primary DNS suffixes*.
11. Click on the *WINS* tab. Select any entries in the *WINS addresses* section of the window, and click on *Remove*. Select the *Default NetBios setting*.
12. Click on *OK*. Click on the *OK* button on the *TCP/IP Properties* screen.
13. Reboot your computer.

For Mac OS 9:

1. Click on the *Apple* icon in the top menu bar. Select *Control Panel > TCP/IP*.



The *TCP/IP* window displays:



2. Select *Connect via Ethernet*. Select *Connect via DHCP*. Leave the other fields blank.
3. Click on the *Close Window* button. The *Save* screen displays:

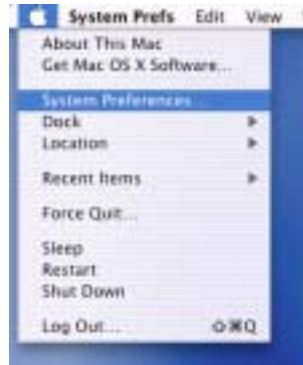


Click on *Save*.

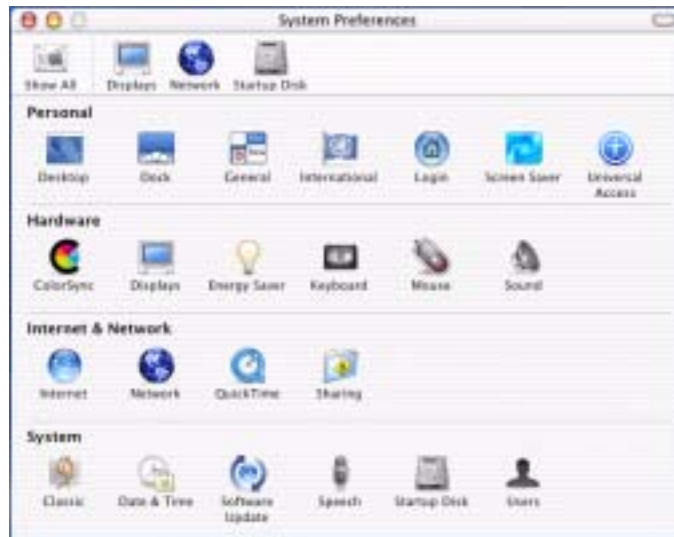
4. If the Internet connection doesn't function immediately, reboot your computer.

For Mac OS X:

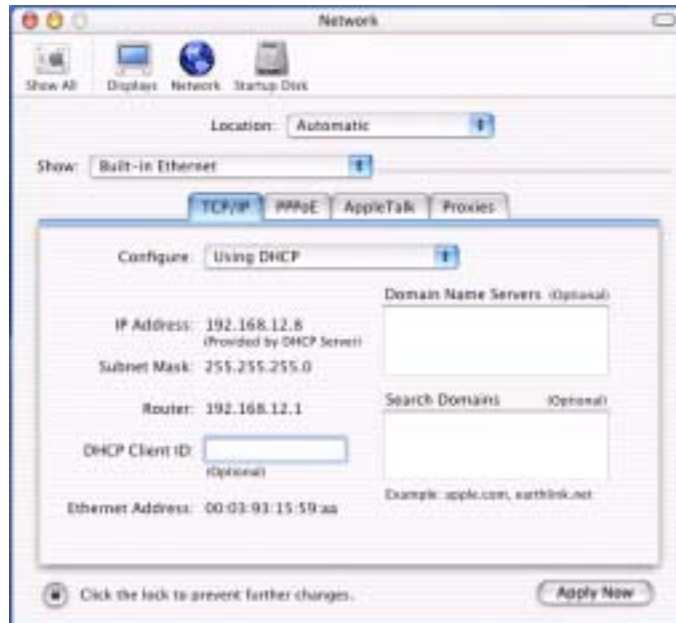
1. Click on the *Apple* icon in the top menu bar. Select *Control Panel > System Preferences*.



The *System Preferences* window displays:



2. Click on the *Network* icon. The *Network* screen displays:



3. Select *Automatic* for location. Select *Built-in Ethernet* for connection. In the *TCP/IP* tab, select the *DHCP* configuration.
4. Click on the *Apply Now* button.
5. If the Internet connection doesn't function immediately, reboot your computer.

Creating an Administrator Account

At this point, your Net Integrator should have an IP address, your workstation should have TCP/IP configured, and both your Net Integrator and your workstation should be connected to the LAN. You now need to create an Administrator account:

1. Open an Internet browser on your workstation. Newer versions of Netscape or Microsoft browsers are recommended.
2. Read the IP address on the display panel. For demonstration purposes, we will use the following address: 192.168.0.1

3. Enter `http://192.168.0.1:8042` into the browser's address bar. Press *Enter* on your keyboard. The *Create Administrator Account* page displays:

Create Administrator Account

Before you can use your Net Integrator, you must create an Administrator Account for yourself. Don't forget your password!

Create Administrator	
User ID:	root
Full Name:	System Administrator
Password:	
Re-enter Password:	
Your Domain Name:	warenet.ru11
Reserve last disk for idb backups?	☒ Yes ☐ No

4. Enter a User ID. The default User ID is *root* – you can use that name or you can create a new ID by typing over the existing text.
5. Enter the administrator's full name.
6. Enter a password.
7. Re-enter your password to ensure it was entered correctly.
8. Enter your organization's registered Internet domain name. Leave the default name if you do not have one, or if you are unsure about whether or not you have one.
9. Indicate whether or not you want to reserve your last disk for idb backup. Refer to *Chapter 23: Disk Management* for more information.
 - Select *Yes* if you want reserve your last disk for idb (while using the other disks for a RAID array).
 - Select *No* if you want to use all available disks for a RAID array.

IMPORTANT: If your Net Integrator has one disk, then you cannot take advantage of idb or RAID. If your Net Integrator has exactly two disks, you can have idb backup **or** a two-disk RAID array (but not both). If your Net Integrator has three or more disks, you can have a two (or more) disk RAID array and idb backup **or** a RAID array with all available disks and no idb backup.

10. Click on the *Save Changes* button. It may take up to a minute for the *Administrator Account Created* page to display:



11. Click on the *Log in* button. Enter your username and password in the WebConfig login screen that displays, and click on the *OK* button. WebConfig's *System Status* screen displays:

Please Note: If you created a RAID array in step 8, the array will now build. The display panel and the *Disk Status* section of the *System Status* screen display the progress of the RAID array. Click on your browser's Refresh button to view an updated status of the RAID array.



SYSTEM STATUS

- SYSTEM STATUS
- USER SETUP
- SOFTWARE UPDATE
- LOGS/REPORTS
- TAKE SNAPSHOT

SERVER SETUP

- FILE
- E-MAIL
- WWW
- FTP
- DNS
- BACKUP

NETWORK SETUP

- LOCAL
- WORKSTATIONS
- PRINTERS
- DIAL-UP
- VPN
- FAST FORWARD

SYSTEM STATUS SNAPSHOT

CPU Utilization:	21%	
Ethernet 0:	2.4 Mbytes/sec	
Ethernet 1:	No traffic - check cabling	
Ethernet 2:	Idle	
PPP Link:	0.0 Mbytes/sec	
Disk Load:	3.4 Mbytes/sec	
Disk Space Used:	48.3 GB / 48.3 GB (90%)	

SERVICES STATUS SNAPSHOT

Internet Status:		1 to 192.168.25.62 - Internet on eth0, via 192.168.20.1
Firewall:		No direct Internet connection. Firewall disabled.
Tunnel Vicious:		Not enabled.
Pure Connection:		Not enabled.
FTTP Connection:		Not enabled.
SoftUpdate:		Idle
Disk Status:		The RAID array is rebuilding. Please do not add or remove any disks until this process is finished (50.9% complete). Disk #7 is being used for Intelligent Disk Backup (IDB). idb disk #7 is不可用。 Update Status
Web Mail:		Available at http://192.168.20.62/mail
Virtual Definition Update:		No valid virtual machine license
Exchange Mail Server:		25 licenses (0 assigned, 25 dynamic)
DNS Server:		Serving local network only
Fast Forward:		0 Sessions CPU Load
WWW Server:		1 Session CPU Load
Secure WWW Server:		1 Session CPU Load
Windows File Server:		0 Sessions CPU Load
Apple File Server:		0 Sessions CPU Load
NFS File Server:		0 Sessions CPU Load
FTP Server:		0 Sessions CPU Load
MySQL Server:		0 Sessions CPU Load
SMTP Server:		0 Sessions CPU Load
IMAP Mail Server:		0 Sessions CPU Load
POP Mail Server:		0 Sessions CPU Load
LDAP Directory Server:		0 Sessions CPU Load

[Reboot](#) [Shutdown](#)

System Status Screen

WebConfig's *System Status* screen displays the status of the services running on your Net Integrator. The WebConfig menu (on the left side of the screen) allows you to access and configure various Net Integrator subsystems.

Features of the System Status screen

CPU Utilization	Displays the utilization of the system's central processing unit (CPU) in numerical form and as a bar graph. During intensive operations (such as backups or very heavy file transfers), the CPU utilization bar might show 100%. <i>This is normal.</i> One hundred per cent utilization simply means that the CPU is being fully utilized and does not necessarily mean that your Net Integrator is being overloaded or that performance will suffer. However, if the CPU utilization is constantly at 100%, and you experience service slow-downs, you might want to contact support for a services review.
Ethernet 0	Displays the speed of data transfer through Ethernet Port 0 (measured in kbps or Mbps). The bar graph displays the speed as a percentage of the highest speed recorded since the last power-up.
Ethernet 1 and 2	Displays the speed of data transfer through the Ethernet Ports 1 and 2 (measured in kbps or Mbps). The bar graph displays the speed as a percentage of the highest speed recorded since the last power-up.
PPP link	Displays the speed of data transfer through the DSL PPPoE or dial-up Internet connection (measured in kbps). The bar graph displays the speed as a percentage of the maximum measured speed.
Disk Load	Displays the amount of data being transferred to and from the hard disk (measured in kbps or Mbps). The bar graph displays the amount as a percentage of the highest amount recorded since the last power-up.
Disk Space Used	Shows how full your Net Integrator hard disk is by displaying the usage and capacity of the drive.

Internet Status	Displays the status of your Internet connection(s). The status light is bright green when an Internet connection is configured properly. The default route used to transfer data to destinations on the Internet also displays. If a modem is configured, clicking on <i>dial modem</i> initiates a connection to the Internet. The administrator can choose to terminate the connection through this screen.
Firewall	Displays the status of the firewall (enabled/disabled).
TunnelVision	Displays the status of all TunnelVision connections.
IPsec Connections	Displays the status of all IPsec connections.
PPTP Connections	Displays the status of all PPTP connections and provides option to disconnect active connections.
SoftUpdate	Displays the status of the subsystem that automatically checks for available software updates. When the subsystem is active and retrieving a list of available software updates, the status light is bright green. When the subsystem is operational but idle, the status light is gray. A red status light indicates a problem with the subsystem (usually an inability to access the distribution server). Refer to <i>Chapter 25: Log Messages</i> for more information on download errors.
Disk Status	Displays the status of your disk configuration, provides disk reconfiguration options, displays the status of a rebuilding RAID array, and displays idb drive hotswap status.
WebMail	Displays the status of the WebMail server, and the address for webmail access.
Virus Definition Updates	Displays whether or not there is a valid virus scanner license, and the last reported update. It also displays when the definitions were last updated, how many viruses you are protected against, and links to a report on how many viruses were detected since the last reboot.
DNS Server	Displays the status of the DNS servers.

FastForward	Displays the status of the port forwarding engine and the number of forwarded sessions. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service. The CPU utilization bar graph indicates how much processor time is being used by this service.
WWW Server	Displays the status of web publishing services. The number of sessions displayed represents the number of active web sessions currently open. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Secure WWW Server	Displays the status of the secure web server. The number of sessions displayed represents the number of active secure web sessions currently open. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Windows File Server	Displays the status of file services for Windows and NT clients. The number of sessions displayed represents the number of active users currently connected to Net Integrator and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
Apple File Server	Displays the status of file services for Apple Macintosh clients. The number of sessions displayed represents the number of users currently connected to Net Integrator and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.

NFS File Server	Displays the status of the NFS file server for UNIX and similar systems. The number of sessions displayed represents the number of active users currently connected to Net Integrator and utilizing file services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
FTP Server	Displays the status of FTP services. The number of sessions displayed represents the number of active FTP downloads currently in progress. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
MySQL Server	Displays the status of MySQL services. The number of sessions displayed represents the number of active users currently connected to the Net Integrator and utilizing MySQL database services. The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
SMTP Server	Displays the status of SMTP services. The number of sessions displayed represents the number of emails being transferred by this server (normally none). The CPU utilization bar graph indicates how much processor time is being used by this service. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.
IMAP and POP3 Server	Displays the status of servers responsible for delivery of email messages from IMAP and POP3 mailboxes. The number of sessions displayed represents the number of users currently downloading email messages from their IMAP or POP3 mailboxes. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service.

LDAP Server	Displays the status of the LDAP server (which is used to publish user names and email addresses into the internal directory). The number of sessions shows how many users are connected. The status light is gray if service is disabled, bright green if service is operational, yellow if service is utilized heavily, and red if there is a problem with the service. The CPU utilization bar graph indicates how much processor time is being used by this service.
Reboot Button	Click on this button to reboot your Net Integrator.
Shutdown Button	Click on this button to properly shut-down your Net Integrator. Failure to click on the <i>Shutdown</i> button means that your RAID array has to rebuild. See <i>Disk Status Messages</i> in <i>Chapter 23: Disk Management</i> for more information.
*Others	Other items may appear on the System Status Screen depending on the addition of any optional software modules. Please refer to the appropriate software documentation for the description of the status indicators.

Configuring your Net Integrator

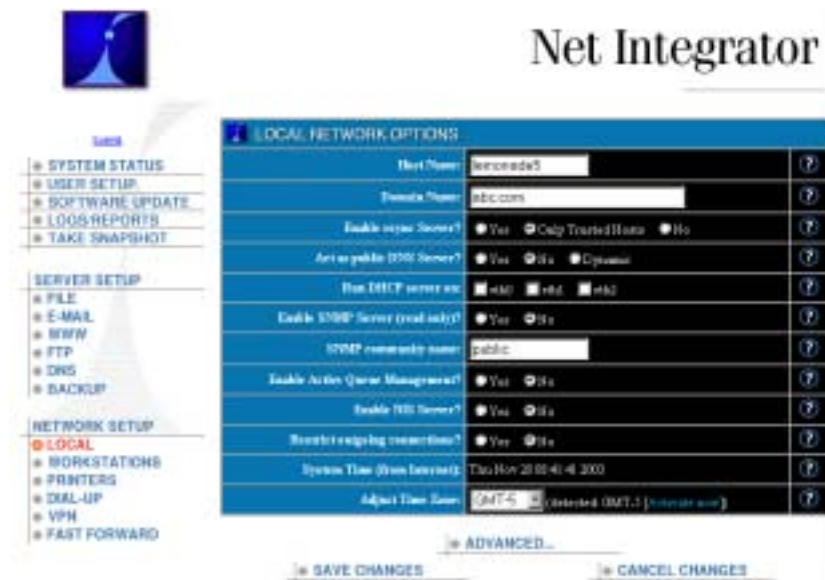
Proceeding with Configuration

You are ready to proceed with the system configuration once you have:

- configured your workstation to use TCP/IP
- created an Administrator account
- logged in and connected to WebConfig

Configuring General Network Settings

1. Select *Local* from the *Network Setup* menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:



2. NetIntelligence automatically assigns a random *Host Name* to the Net Integrator during the first boot-up. If appropriate, enter a new host name by typing over the existing text. The new host name should be unique, it should use only numbers and letters, and it should contain no spaces.

Please Note: Host Names should be unique because they are used to distinguish your box from others on the local network and are used by local users to identify a Net Integrator's file and print-sharing resources. In addition, the host name (in conjunction with the domain name) forms a unique Internet name under which the Net Integrator and its web, FTP, and email services are addressed on the Internet.

3. If appropriate, enter a new domain name by typing over the existing text.

Please Note: Domain Names are part of the Internet naming standard (which applies to every device connected to the Internet). Each host has a unique name, which consists of a host name and domain name. In general, all Internet hosts owned by your company will belong under the same domain.
4. Indicate whether or not you want the *rsync server* to be enabled. This options is for Unix-style clients only. We recommend that you leave the default setting.
5. Select the appropriate public DNS resolution option.
 - Select *Yes* if you want Net Integrator to perform DNS resolution for Internet hosts.
 - Select *No* if you do not want Net Integrator to perform DNS resolution.
 - Select *Dynamic* if you want Net Integrator to perform Dynamic DNS resolution.

Please Note: If the public DNS server is enabled, Internet hosts can resolve name-to-IP number queries for Internet services provided by Net Integrator. Dynamic DNS resolution allows you to host email, web, and FTP services using an Internet connection with a dynamic IP address.

6. The DHCP server is set by default to “turned off” on eth0, if no other DHCP server is on that segment. We recommend that you turn this on.
7. Indicate whether or not you want to enable the SNMP (Simple Network Management Protocol) server.

Please Note: SNMP is used to collect statistical information from the host about parameters such as network throughput and CPU utilization. It is also used for network monitoring.

8. If you enable the SNMP server, enter an appropriate SNMP community name.
9. Choose whether or not to enable Active Queue Management. Active Queue Management, also known as traffic shaping, allows smoother division of network traffic between high-bandwidth connections (like large file downloads) and low-latency connections (like telnet). It also works better with some ISPs that download slowly when you are uploading data.
10. Indicate whether or not you want to enable the NIS Server. Leave NIS disabled if you are using Windows. If you are using Unix or a similar system, leave it disabled unless you need NIS Service.
Please Note: Net Integrator's built-in Network Information Server (NIS) is used to share usernames and groups across a network to simplify user access. Unix and similar systems can be configured to use NIS. Net Integrator uses NIS version 2.
11. Choose whether or not to Restrict Outgoing Connections. As part of the Net Integrator's ICSA compliance, the Net Integrator can restrict outgoing connections to a few protocols. Enabling this option allows outgoing traffic based on the server's configuration. All other traffic will be blocked. See *Chapter 19: Firewall Services* for more information.
12. The Net Integrator synchronizes its clock from a source on the Internet. To set the proper time, select your Time Zone from the drop-down list. The Net Integrator will attempt to auto detect the proper time-zone and display its detected results for you.
13. Click on the *Save Changes* button.

Configuring Advanced Network Settings

The *Advanced Network Settings* screen allows you to configure some of Net Integrator's more advanced features. Changing advanced network settings can cause odd behavior on your network; for example, if you change Net Integrator's IP address or Netmask to an incorrect value, you may not be able to reach it from your web browser to change it back. If something goes wrong with these settings, you have to use the control panel on the front of the server to change them back.

Please Note: If you intend to use TunnelVision (discussed in *Chapter 16*), every network in each office location that will be connected through a VPN must have a separate network subnet. If Net Integrator boxes in various locations auto-configure their local network interfaces to the same subnet, you will have to change your subnet number and IP address to a different value. Refer to *Reconfiguring Network Devices* in this chapter for information on how to do that.

Advanced Network Settings screen

To access the *Advanced Network Settings* screen:

1. Select *Local* from the *Network Status* menu found on the left side of any WebConfig screen. The *Local Network Options* screen displays.
2. Select the *Advanced...* option at the bottom of the screen. The *Advanced Network Settings* screen displays:

NETWORK DEVICES					
Device	IP Address	Netmask	Mode	Trust?	Action
eth0	192.168.12.10	255.255.255.0	DHCP	Yes	...
eth1	64.12.25.161	255.255.255.0	Forced (User)	Yes	...
eth2	0.0.0.0	0.0.0.0	NetMap	Yes	...

NETWORK ROUTES		
Destination	Gateway	Action
192.168.12.0/24	Direct to eth0	... X
64.12.25.0/24	Direct to eth1	... X
Default	via 192.168.12.1 on eth0	... X

[ADD NEW ROUTE](#)
[HOME](#)

Network Devices

The following list describes the *Network Devices* section of the screen:

- **Device** – lists the network interfaces installed on Net Integrator. *Eth0* should be connected to your LAN. *Eth1*, *Eth2*, and *PPP0* should be connected to the Internet.
- **IP Address** – lists the IP addresses to the interfaces.
- **Netmask** – lists the IP network mask assigned to a particular interface.
- **Mode** – describes how an IP address was assigned to an interface.
 - *Forced* means that a permanent IP address was assigned by an administrator. *Eth0* should always have a forced IP address.
 - *DHCP* means that a temporary IP address was assigned by the DHCP server. DHCP addresses change each time you turn-on your Net Integrator.

- *NetMap* indicates that the IP address was automatically assigned by your Net Integrator.
- **Trust** – a very important parameter. *Yes* signifies a trusting relationship with all hosts attached to that interface (meaning that **no firewall protection is applied to that interface**). *Eth0* should always be configured as trusted. *No* means that any traffic arriving at that interface is considered non-trusted; as such, appropriate firewall protection is applied. All Internet connections should be configured as non-trusted.
- **Action Button** – Clicking this button displays a screen where interface settings can be changed.

Reconfiguring Network Devices

1. Click on an interface's *Action* button.
2. The *Network Settings* screen for that interface displays:

Network Settings for eth0		
IP Address:	192.168.212.1	?
Netmask:	255.255.255.0	?
Trust computers on this network (pass them through the firewall)?	☒ Yes ☐ No	?
Choose address automatically?	☒ Yes ☐ No	?
DHCP Client ID (leave blank to use hostname):		?
Use default gateway on this link?	☒ Yes ☐ Only as last resort	?
<input checked="" type="button" value="SAVE CHANGES"/> CANCEL CHANGES		

3. **Optional:** Enter a new IP address (in the format 192 . 168 . 12 . 10).
4. **Optional:** Enter a new network mask (in the format 255 . 255 . 255 . 0).
5. **Optional:** Indicate whether or not to trust computers on this network.
6. **Optional:** Indicate whether or not you want the Net Integrator to automatically choose an IP address and network mask.
 - The default setting is *Yes*, meaning that the Net Integrator automatically selects an IP address and network mask.
 - The default setting is changed to *No* (and autoconfiguration is disabled) if you entered a new IP address or a new network mask and clicked on the *Save Changes* button.

Please Note: *Eth0* should never be set to choose automatically. Once an IP has been chosen, the interface should have its option forced (not automatic) unless you are running a separate DHCP server on the local network.

7. **Optional:** If your DHCP server (i.e. your cable modem provider) specified that you need a DHCP Client ID when setting up your network, enter it here.
8. **Optional:** Indicate whether or not you want the Net Integrator to use this link as the default gateway.
 - If this is set to *Yes*, Net Integrator will create a default route to the network through this interface at the highest priority level, so this link will be used by default for incoming and outgoing traffic.
 - If this is set to *Only as last resort*, Net Integrator will create a default route to the network through this interface with a lower priority level, so it will be used only if your higher-priority ("Yes") links stop working.
9. Click on the *Save Changes* button.

Network Routes

The *Network Routes* section of the screen displays the IP routes known to the Net Integrator. Because Net Integrator automatically discovers its network surroundings and sets up routing tables, you generally do not need to edit them. However, depending on your Internet connection, your ISP *may* assign you a new route (in which case you have to edit the default route).

Please Note: Whether or not you have to change any route settings depends on your network setup and Net Integrator's connection to the LAN and to the Internet.

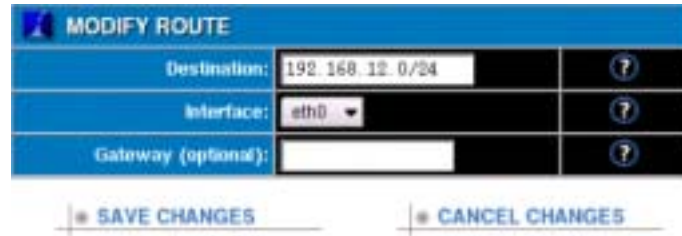
Deleting Network Routes

1. Click on the appropriate route's *Delete* button.
2. In the window that appears, confirm the deletion by clicking on the *Ok* button.

Please Note: If the server prevents the route from being deleted, the server deems the route as "required" or important, as it must relate to another setting or subnet in your "Device" list. If you continue to have issues, review FAQs for a "Netscan" option or contact support.

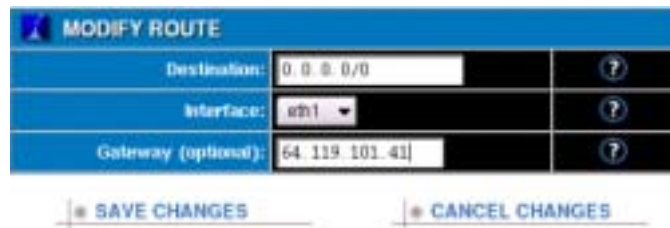
Editing Network Routes

1. Click on the appropriate route's *Action* button. The following screen displays:



The screenshot shows a web form titled "MODIFY ROUTE". It contains three input fields: "Destination:" with the value "192.168.12.0/24", "Interface:" with a dropdown menu showing "eth0", and "Gateway (optional):" which is empty. Each field has a help icon (a question mark in a circle) to its right. At the bottom of the form are two buttons: "SAVE CHANGES" and "CANCEL CHANGES".

2. **Optional:** Enter a new destination IP address and netmask (in the format 192.168.12.0/24).
3. **Optional:** Click on the *Interface* drop-down arrow and select the interface over which this network can be accessed.
4. **Optional:** If this is not a local network route entry (i.e. *eth1* or *eth2*), enter the network's gateway address:

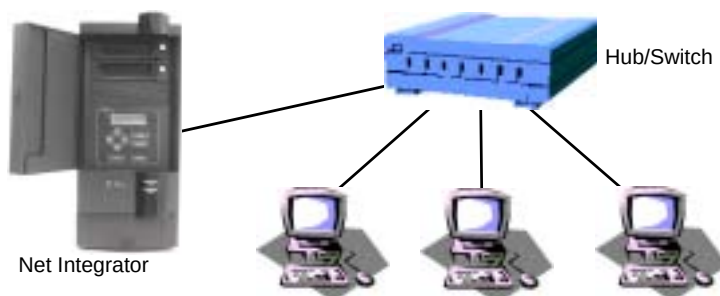


The screenshot shows the same "MODIFY ROUTE" form, but with different values. The "Destination:" field now contains "0.0.0.0/0", the "Interface:" dropdown menu shows "eth1", and the "Gateway (optional):" field now contains "64.119.101.41". The "SAVE CHANGES" and "CANCEL CHANGES" buttons are still at the bottom.

5. Click on the *Save Changes* button.

Network Configuration Scenarios

1. Net Integrator as a Workgroup Server without a direct connection to the Internet



In this scenario, you would go to the *Advanced Network Settings* screen to change the IP address or the network mask of the local network interface or Net Integrator's default route. Although you generally do not need to change these settings, you can still do so:

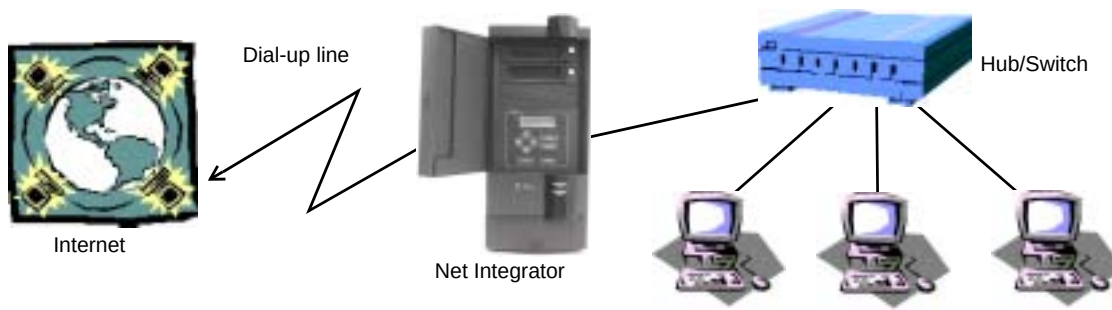
- a. In the *Network Devices* or *Network Routes* section of the *Advanced Network Settings* screen, click on the appropriate *Action* button.
- b. Depending on your choice, the *Modify Route* or the *Network Settings* screen displays:
Please Note: Refer to *Reconfiguring Network Devices* and *Editing Network Routes* earlier in this chapter for full descriptions of these two screens.

The first screenshot is the 'MODIFY ROUTE' screen. It has a blue header with a question mark icon and the title 'MODIFY ROUTE'. Below the header are three input fields: 'Destination:' with the value '192.168.12.0/24', 'Interface:' with a dropdown menu showing 'e0/0', and 'Gateway (optional):' which is empty. Each field has a question mark icon to its right. At the bottom are two buttons: 'SAVE CHANGES' and 'CANCEL CHANGES'.

The second screenshot is the 'Network Settings for e0/0' screen. It has a blue header with a question mark icon and the title 'Network Settings for e0/0'. Below the header are several settings: 'IP Address:' with the value '192.168.212.1', 'Network Mask:' with the value '255.255.255.0', and three radio button options: 'Treat computers on this network (yes/no) through the firewall?' (Yes selected), 'Choose address automatically?' (Yes selected), and 'DHCP Client ID (leave blank to use hostname):'. Each setting has a question mark icon to its right. At the bottom are two buttons: 'SAVE CHANGES' and 'CANCEL CHANGES'.

- c. Change the appropriate settings and click on the *Save Changes* button.

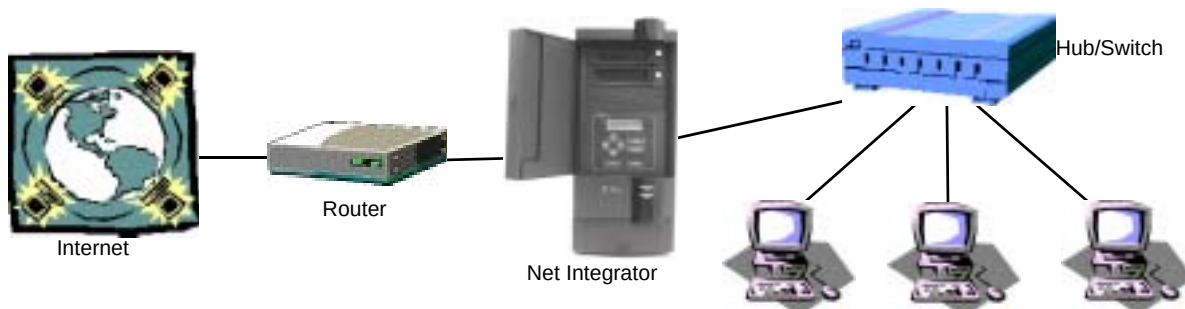
2. Net Integrator as a Workgroup Server and Dial-up Gateway to the Internet



If the Net Integrator has automatically chosen the proper IP addresses, there is nothing else for you to change. If you want to change the Net Integrator local IP addresses, you can do so by clicking the *Edit* button on the line describing the parameters for the Ethernet 0 interface.

The default route is automatically determined when Net Integrator dials in to the Internet. In this case, there should be no default route entry in the Routes Table.

3. Net Integrator as a Workgroup Server and High-speed Gateway to the Internet



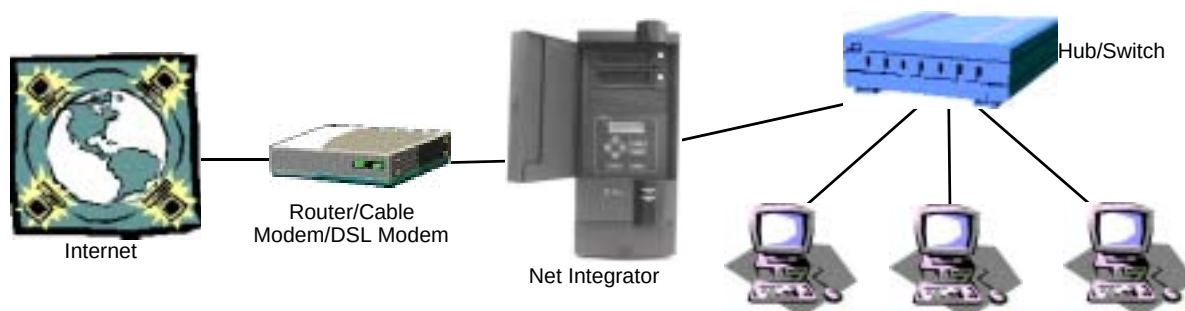
Net Integrator auto configures its parameters if the ISP uses DHCP as a means of automatic network configuration. In this case, there should be nothing for you to do on the *Advanced Network Setup* screen (although you can change the address of your local network interface if you wish to do so).

If your ISP assigns a unique static IP address, network mask, and default route, Net Integrator will likely discover the proper default route but will not know which IP address to select. Although Net Integrator will find the available address and establish a proper con-

nection to the Internet, you should change the IP address of your Internet interface to the address assigned by your ISP. You should do the same with the default route setting. If you run into problems configuring advanced network settings, contact technical support. To change these settings:

- a. In the *Network Devices* section of the *Advanced Network Settings* screen, click on the *eth1 Action* button.
- b. The *Network Settings* screen displays. Enter the new IP address and click on the *Save Changes* button.
- c. In the *Network Routes* section of the *Advanced Network Settings* screen, click on the *Default Action* button (the last entry in the list).
- d. The *Modify Route* screen displays. Change the default route and click on the *Save Changes* button.

4. Net Integrator as a Domain Controller and High-speed Gateway to the Internet



Net Integrator can serve as a Windows NT style domain controller for all the computers running Windows on the network. As the domain controller, Net Integrator will provide authentication services for the computers on the network. When this function is enabled, the Windows file server is set up as a domain controller, and a domain will replace the Windows workgroup. For specific information on configuring domain controllers, please see *Chapter 7: Domain Controller*.

Configuring your Internet Connection

Configuring a Dial-up Modem

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays:

Device	Type	Allow Connect?	Allow Dial-In?	Action
ADSL/PPPoE/PTT on stb	PPPoE-Ethernet or PPTP (often used on ADSL line)			...
ADSL/PPPoE/PTT on stb	PPPoE-Ethernet or PPTP (often used on ADSL line)			...
ADSL/PPPoE/PTT on stb	PPPoE-Ethernet or PPTP (often used on ADSL line)			...
Modem #1	Dial-up PPP	*		...

* DETECT MODEMS

2. **Optional:** If you have an external modem connected, you may need to click on the *Detect Modems* button to initiate the Modem Detection Cycle. Refer to *Chapter 4: DoubleVision* for information on using multiple dial-up modems.

Please Note: If modem undetected, check cables/power, etc. Cycle power on modem and initiate a new *Detect Modems* test. Refer to FAQ for more troubleshooting tips.

3. Click on the *Modem #1 Action* button. The following screen displays:

DIAL-UP NETWORKING SETUP	
Type of connection:	Point-to-Point Protocol (PPP) using a standard phone line
Internet Provider's Phone Number:	?
Internet Account Username:	?
Account Password:	?
Re-enter Password:	?
ADVANCED OPTIONS	
Disconnect when idle for how many seconds?	300 ?
Dial automatically when someone tries to reach the Internet?	☒ Yes ☐ Only as a last resort ☐ No ?
Enable Windows Dial-up Networking?	☒ Yes ☐ No ?
Allow Dial-in connections?	☒ Yes ☐ No ?

* SAVE CHANGES * CANCEL CHANGES

4. Enter the phone number provided by your ISP. If you have to dial 9 to get an outside line, enter this number as well. For example, enter: 9, 123-123-1234.

5. Enter the Internet account username provided by your ISP.
6. Enter the account password provided by your ISP.
7. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
8. Indicate the number of idle seconds before automatic disconnection.
Please Note: If you enter zero, the connection will never automatically disconnect. Be careful with this setting, especially if you do not have an unlimited Internet access package from your ISP.
9. Select the appropriate dialing mode:
 - Select *Yes* if you want the Net Integrator to dial automatically to the Internet when someone tries to reach it.
 - Select *No* if you want to manually initiate a connection by clicking *Dial Modem* on the *System Status* page.
 - Select *Only as a last resort* if you want to use a dial-up connection when one or more of your high-speed connections fail. The dial-up connection will stay active until one of the high-speed connections becomes functional. Although all traffic is forwarded to the high-speed connection when it returns to normal, the dial-up connection remains active for a few minutes in case the high-speed connection fails again. In that case, the system re-routes traffic back to the dial-up connection immediately without having to wait for a dial-up connection to be re-established.
10. Indicate whether or not you want your Net Integrator to emulate *Windows Dial-up Networking*.
Please Note: Some Internet providers are setup to work only with Windows dial-up clients. If you have problems establishing dial-up connection, try enabling this option.
11. Indicate whether or not users will be able to establish a remote dial-in modem connection to the internal network.
Please Note: A user's VPN (PPTP) and Dial-In access has to be enabled before they can establish a remote connection. See *Creating Users* in *Chapter 5: User & Team Management* for more information.
12. Click on the *Save Changes* button.

Configuring a DSL Connection (PPPoE)

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays.
2. Click on the *Action* button in the appropriate ADSL row (eth1 or eth2 only). The *ADSL Dialer Options* screen displays:

ADSL Dialer Options		
Type of connection:	PPP-over-Ethernet (PPPoE) or PPTP, often used on ADSL lines	
Internet Account Username:		?
Account Password:		?
Re-enter Password:		
Gateway IP (leave blank if unknown):		
Enable this connection:	☒ Yes ☐ Only as a last resort ☐ No	
SAVE CHANGES		CANCEL CHANGES

3. Enter the Internet account username provided by your ISP.
4. Enter the account password provided by your ISP.
5. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
6. **Optional:** Enter your gateway IP address. Leave this blank if you don't know the address.
7. Indicate whether or not you want to enable the connection.
 - Select *Yes* if you want to establish a permanent connection.
 - Select *No* if you do not want to establish a connection.
 - Select *Only as a last resort* if you want to use this connection only if the primary connection fails.
8. Click on the *Save Changes* button.

Configuring a Leased Line Connection

1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays.
2. Click on the *Leased Line Action* button. The following screen displays:

Leased Line PPP Options	
Type of connection:	PPP over X.21 (or v.35), often used on a leased line
Internet Account Username:	testuser
Account Password:	*****
Re-enter Password:	*****
Enable this connection:	☒ Yes ☐ Only as a last resort ☐ No

3. Enter the account username provided by your ISP.
4. Enter the account password provided by your ISP.
5. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter your password in both fields.
6. Indicate whether or not you want to enable this connection.
 - Select *Yes* if you want to establish a permanent connection using the leased line. This is the recommended setting.
 - Select *No* if you do not want to establish a connection using the leased line.
 - Select *Only as a last resort* if you want to use the leased line connection only if the primary connection fails.
7. Click on the *Save Changes* button.

Take A Snapshot

Now that you have taken the time to configure your Net Integrator you can use the *Take Snapshot* item in the left hand menu to display all the information available on one scrollable page.

What is DoubleVision?

DoubleVision is a Net Integrator feature that allows you to configure two or more Internet connections. For example, you can combine a cable modem and an ADSL link, two ADSL links, multiple dial-up modems (to the same or different ISP), or any combination of Internet connections supported by Net Integrator.

There is no single place to configure DoubleVision. Instead, it is automatically configured when more than one Internet connection is used at the same time.

Please Note: In order for *DoubleVision* to activate, you must have at least two gateway connections. You can choose a default connection.

Advantages to DoubleVision

- **Increased performance**

Internet traffic is increased by being able to utilize the bandwidth of both lines.

Please Note: You cannot specify which connection is used. It is automatically chosen by *NetIntelligence*.

- **Increased reliability**

If one ISP's Internet connections fails, the remaining ISP's connection stays functional. This means that your downtime is limited (it's also known as fail-over, or redundant connectivity).

- **Last Resort dial-up mode**

If one or more of your high-speed Internet connections fail, Net Integrator can dial your modem automatically and use dial-up access instead. When your high-speed links are restored, the modem automatically disconnects after it verifies that the high-speed connections are stable and active. The same applies to high-speed connections if you choose to use them as a last resort connection.

- **Dynamic DNS Integration**

If you're using Dynamic DNS, the Net Integrator automatically publishes appropriate DNS names so that people can always find your web site, even if your high speed links are down and you need to use a dial-up connection. See *Chapter 20: Domain Name Services* for more information.

- **NetIntelligence**

No human intervention is required to activate and deactivate Internet services when they fail or are restored. NetIntelligence automatically takes care of these situations.

- **Full automation**

You do not have to reconfigure any client workstations on your local network in order to take advantage of DoubleVision. DoubleVision is fully automated and managed by the server.

Modem Connections

Since modems are normally much slower than other Internet connections, you probably do not want to use a modem as your primary connection. Instead, you can configure your modem as a 'last resort' option, meaning that your modem will only connect if one or more of the high-speed connections fails.

If a modem is configured as the primary connection, it will connect to the Internet even if high-speed connections are available. This is useful if you want to test the modem connection.

User & Team Management

Service Integration

User and team management is tightly integrated with a number of other Net Integrator services. It is **very important** that you understand how user and team management relates to these other functions before we start talking about creating, editing, and deleting users and teams. Please read the following section carefully.

Net Integrator's email, file, web, and FTP services are tightly integrated. Every user and team account that is created has instant and automatic access to all of these services. When a user is created, a number of things happen in the background:

- a login account is created and the password defined by the administrator is assigned to that account.
- a personal user directory is created on the server. This directory is accessible in Windows' Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/username` to access this directory. For example, the path for someone with the username *janedoe* would be `/export/home/janedoe`.
- a WWW directory is created within the user's personal directory. Any file stored in this directory is automatically published on the user's personal web page.
- an FTP account (which points directly to the user's personal directory) is created for the user. If the user logs in to the FTP server using the proper user name and password, they can access the files in their personal directory.
- an email account is created for the user. Email is available through either POP3, IMAP, or WebMail.

Similarly, when a team is created, a number of things happen in the background:

- a team login account is created and the password defined by the administrator is assigned to that account.
- a team directory is created. This directory is accessible to all team members in Window's Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/teamname`

to access this directory. For example, the path for a team named *sales* would be */export/home/sales*.

- a WWW directory is created within the team directory. Any file stored in this directory is automatically published on the team's web page.
- an FTP account (which points directly to the team directory) is created for the team. If a team member logs into the FTP server using the proper team name and password, they can access the files in the team directory.
- an email distribution account is created for members of the team. Team email can be accessed through either POP3 or IMAP mailboxes. Emails received by the team email account may be set to be automatically forwarded to all members of the team.

User Accounts

Creating Users

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main Setup* screen displays:

TEAM SETUP							
Admin	Team ID	Full Name	Members	FTTP/Dial In	FTP		Action
exchangel-admin		Exchange(T) Server Administrator					...
ftp		Anonymous FTP Admin					...
log		System Log Files					...
maildir		Database for mailing list archives					...
webmaster		Web Server Admin					...
USER SETUP							
Admin	User ID	Full Name	Teams	FTTP/Dial In	FTP	Exchange(T)	Action
*	root	System Administrator			*		...
* ADD NEW USER		* ADD NEW TEAM		* IMPORT USERS			

- Click on the *Add New User* button. The *Create New User* screen displays:

- Enter the User ID that will serve as the user's login and personal directory name. User IDs cannot contain spaces or any punctuation other than the hyphen, the dot, or the underscore (e.g. *jane-doe*, *jane.doe*, *janedoe*).
Please Note: If Net Integrator's email server is used to receive email, this user ID will become part of the user's email address. For example, if the username *janedoe* is created on a Net Integrator that resides in the *example.com* domain, Jane's email address will be *janedoe@example.com*.
- Enter the user's full name.
- Enter a password for the user. User passwords should be unique.
- Re-enter the password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter the password in both fields.
- Indicate whether or not this user will have administrative privileges. Administration privileges means that this user will have unrestricted access to all configuration functions of Net Integrator.
- Indicate whether or not this user will have FTP access to his or her private directory.
Please Note: FTP has to be enabled before the user has FTP access. If FTP is enabled in *Trusted Hosts Only* mode, the user can access files from a trusted, internal network or from a VPN. If FTP is enabled in open mode, the user can access files using FTP from anywhere on the Internet.
- Indicate whether or not the user is allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most users should not be able to establish a remote connection.
Please Note: VPN services have to be enabled before a user can establish a VPN connection. Similarly, dial-in for a specific modem has to be enabled before a user can establish a dial-in connection on that modem. See *Chapter 18: Remote Access Services* for more information.

10. If the domain controller is enabled, choose a drive that the user's files can be automatically mounted to when logged into a domain workstation. The default drive is X:.
Please Note: Be sure to choose a drive that is not already in use. For more information, see *Chapter 7: Domain Controller*.
11. Select the teams this user will be a part of. Team membership gives users full access to the team's shared directory.
12. Click on the *Save Changes* button. The *Main User Setup* page re-displays, and the user displays in the list of previously created users.

Editing Users

1. On the *Main User Setup* screen, click on the appropriate user's *Edit Action* button. The *Modify User* screen displays:

User ID:	DEV/USER	?
Full Name:	Any User	
Password:	password	
Re-enter Password:	password	
Administrator Access:	☒ Yes ☐ No	?
Allow FTP Access:	☐ Yes ☒ No	?
Allow VTN (FTP) and Dial-In Access:	☐ Yes ☒ No	?
Allocate Exchange/IM License:	☒ Yes ☐ No	?
Automatically mount files on:	X:	?
Join Teams:	☐ backup ☐ exchange-admin ☐ log ☐ mailbox ☐ netlogon ☐ postmaster ☐ webmaster	?
Test E-Mail:	[Send]	?

2. Change the user's information as appropriate. Refer to *Creating Users* (in this chapter) for a description of the fields on this screen.
3. Click on *Convert to Team* to convert this user into a team.
4. Click on the *Saves Changes* button.

Deleting Users

IMPORTANT: Deleting a user means that all of the user's personal files, email settings, mailbox, and any undelivered email in the mailbox will be deleted. Once this is done, none of the above can be recovered (unless you restore the data from a previous backup).

1. On the *Main User Setup* screen, click on the appropriate user's *Delete* button.
2. A "delete user" confirmation box appears. Select the *OK* button to continue and **DELETE** the user.

Import Users from Windows

To upload user information from a Windows 2000 or NT server:

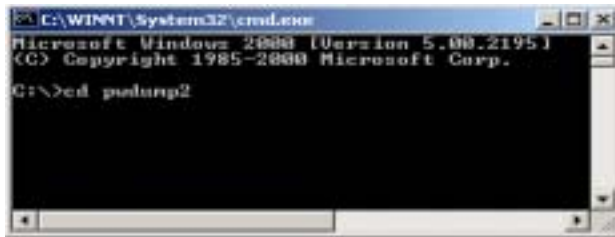
1. You will need to download an executable file called "pwdump2". The program is freely available online and can be found at various locations on the Internet. Here is one: http://razor.bindview.com/tools/desc/pwdump2_readme.html
2. Download the file called "pwdump2.zip" and unzip the contents to their own folder. For example, extract the contents to a folder called "pwdump2" on your C drive.
3. Click on the *Start* menu, and choose *Run*.



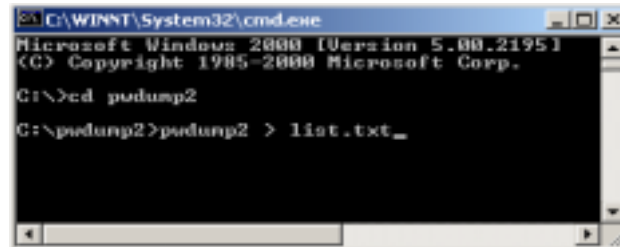
4. Enter “cmd” and click *OK*.



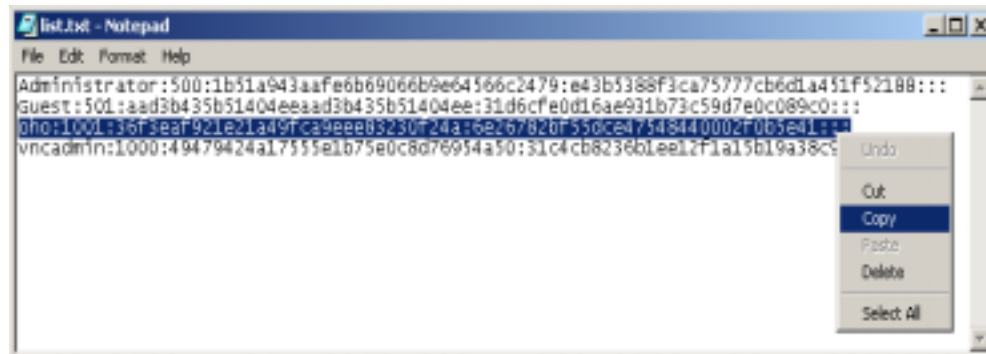
5. Type “cd pwdump2” and hit *Enter*. This will change the directory to the folder you created on your C drive that contains the contents to the file “pwdump2.zip”.



6. Type “pwdump2 > list.txt” and hit *Enter*. This will run the file called “pwdump2.exe” and generate a text file called “list.txt” in the same folder.



- Open the file called “list.txt”. This contains a list of Windows users. Highlight the users you wish to import, right-click with your mouse and choose *Copy*.



- In WebConfig, click on *User Setup* in the left-side menu.



- Click on *Import Users*. This screen will display.



10. Right-click on your mouse in the field called “Import Users Info”. Choose *Paste*. This will copy the contents of the file called “list.txt” into this space.



11. Click on *Save Changes*. This screen will display.



12. Click on *Save Changes*.
13. Because windows utilizes a one-way hash algorithm for storage of passwords, the passwords are not easily recovered. The Administrator will need to create new passwords by

clicking on the left button in the *Action* column, in the row containing a user's information. This screen will display:

MODIFY USER	
User ID:	myuser ?
Full Name:	Any User ?
Password:	password ?
Re-enter Password:	password ?
Administrator Access:	☒ Yes ☐ No ?
Allow FTP Access:	☐ Yes ☒ No ?
Allow VPN (PPTP) and Dial-In Access:	☐ Yes ☒ No ?
Allocate Exchange IM License:	☒ Yes ☐ No ?
Automatically mount file net:	☐ ?
Join Teams:	☐ backup ☐ exchange-admin ☐ log ☐ mailbox ☐ maillogon ☐ postmaster ☐ webmaster ?
Test E-Mail:	test ?

14. Enter the new password into the appropriate fields. Click *Save Changes*.

Modifying User Email Settings

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.
2. Click on the appropriate user's *Action* button. The *Modify Users* screen displays.

- Click on the *E-mail...* button on the bottom of the screen. The *E-mail Setup* screen displays:

The screenshot shows the 'E-MAIL SETUP' window. It has a blue header bar with the title 'E-MAIL SETUP'. Below the header, there are several input fields and checkboxes. Annotations A, B, C, and D point to specific fields:

- A** points to the 'Retrieve Mail from POP Server:' field, which contains 'mail.example.com'.
- B** points to the 'Remote POP Username:' field, which contains 'remoteuser'.
- C** points to the 'Keep Mail if Forwarding?' checkbox, which is checked.
- D** points to the 'Automatic Reply Message' text area, which is empty.

At the bottom of the window, there are two buttons: 'SAVE CHANGES' and 'CANCEL CHANGES'.

Section A:

- Retrieve Mail from POP Server:
 - Used to POP mail from your current mail provider and/or used to pull third party POP mail (i.e. Yahoo/Hotmail).
 - Configure by entering the full server name used to pull mail down from your ISP (i.e. pop1sympatico.ca).
- Remote POP Username:
 - Enter the appropriate account credentials for the mail service you are retrieving from.
- Remote POP Password:
 - Enter password for POP account.
- Re-enter POP Password:
 - Re-enter password for POP account.

Section B:

1. Forward to this E-Mail Address:
 - This is a “by user” mail forwarder. This allows you to forward or send copies of your mail to an alternative address (e.g. you’re leaving for vacation, but need your colleague to review your email for sales orders).

Section C:

1. Keep Mail if Forwarding?:
 - Gives you the ability to keep a copy of all the mail that you have forwarded for later review or archive.
 - Default setting is YES.

Section D:

1. Automatic Reply Message:
 - Also known as the “Out of Office” notification.
 - Users can automate a private reply message for any mail that gets sent to them.

Please Note: This feature is intelligent and is designed to send a single response to each address that gets received to your mailbox. If the same user sends you ten messages, they will only receive one auto reply from your mailserver.

Team Accounts

Creating Teams

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.

- Click on the *Add New Team* button. The *Create New Team* screen displays:

- Enter a team ID. This ID serves as the name of the team's shared directory and as the team's FTP login name (which gives team members FTP access to the shared directory and the WWW directory). Team IDs cannot contain spaces or any punctuation other than the hyphen, the dot, or the underscore (e.g. *sales-team*, *sales.team*, *sales_team*).
- Enter a descriptive name for the team in the *Full Name* field.
- Enter a login password for the team. Team passwords should be unique.
- Re-enter the password to ensure it was entered correctly. If the passwords do not match, you will be asked to re-enter the password in both fields.
- Indicate whether or not the team will have FTP access to the team directory.
Please Note: FTP has to be enabled before the team has FTP access. If FTP is enabled in *Trusted Hosts Only* mode, the team can access files from the internal network or from a VPN. If FTP is enabled in open mode, the team can access files using FTP from anywhere on the Internet.
- Indicate whether or not team members are allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most teams should not be able to establish a remote connection.
Please Note: VPN services and dial-in services have to be enabled before a team member can establish a VPN or dial-in connection. See *Chapter 18: Remote Access Services* for more information.
- Select the appropriate group email setting:
 - Select *Send to members* to send team emails to all team members.

- Select *Use shared folder* to store all team emails in an automatically created folder that is accessible to all team members through an IMAP client.
- Select *Act as mailing list* to make the group email address act as a mailing list where others (even non-group members) can subscribe.

When a mailing list is first set up, no one is subscribed to it. People who want to subscribe (including group members) must do it themselves. To subscribe/unsubscribe, mail is sent to `group-subscribe@example.com` or `group-unsubscribe@example.com`.

The mail list files are maintained in the group's home directory under `Maildir/list-mail/`.

The default value for a group email is to forward mail to all members.

10. If the domain controller is enabled, choose a drive that the team's shared files can be automatically mounted to when one of its members logs into a domain workstation. The default, *None*, does not mount the files to ensure that there are no conflicts with drive space.
Please Note: For more information, see *Chapter 7: Domain Controller*.
11. Select the members of the team. Team membership gives full access to the team's shared directory.
12. Click on the *Save Changes* button. The *Main User Setup* page re-displays. The team displays in the list of previously created teams.

Editing Teams

1. On the *Main User Setup* screen, click on the appropriate team's *Action* button.
2. The *Modify Team* screen displays:

3. Change team information as appropriate. Refer to *Creating Teams* (in this chapter for a description of the fields on this screen).
4. Click on *Send* to send this team a test email.
5. Click on *Convert to User* to convert this team into a user.
6. Click on the *Save Changes* button.

Convert to User

Clicking on “*Convert to User*” on the *Modify User* screen will convert a “user” into a team of the same name.

Convert to Team

Clicking on “*Convert to Team*” on the *Modify User* screen will convert a team into a user account. All team members will be removed.

Deleting Teams

IMPORTANT:Deleting a team means that the team’s shared network directory and all of the files contained within the directory are deleted. Once this is done, none of the above can be recovered (unless you restore the data from a previous backup).

1. On the *Main User Setup* screen, click on the appropriate team’s *Delete* button.
2. In the window that displays, click on the *OK* button.

File Sharing Services

Net Integrator is designed to provide high performance file sharing services for Windows, Macintosh, and UNIX-style clients. Files created by Windows users can transparently be seen by Macintosh users and vice versa.

The management and administration of file services is tightly integrated with user management and administration. Please refer to *Service Integration* in *Chapter 5: User & Team Management* for a detailed explanation of how file sharing services are automatically setup during user and team creation.

Configuring File Services

1. Select the *File* from the *Server Setup* menu on the left side of any WebConfig screen. The *File Server Setup* screen displays:

FILE SERVER SETUP		
Enable File Virus Scanner?	☒ Yes ☐ No	?
Enable Macintosh file server?	☐ Yes ☒ No	?
Enable Windows file server?	☐ Yes ☒ No	?
Windows working group name:	WORKGROUP	?
Enable Domain Controller for Windows?	☒ Yes ☐ No	?
Domain Controller: Enable roaming profiles?	☐ Yes ☒ No	?
Domain Controller: Admin password (username is _root):		?
Domain Controller: No enter admin password:		
Enable NFS file server?	☐ Yes ☒ No	?
Mapping scheme for NFS:	☒ upidd ☐ None	?

FILE SYNC...

SAVE CHANGES CANCEL CHANGES

2. If appropriate, enable the Macintosh File Server. If Macintosh file services are not enabled, users will not have access to their personal network directories or shared team directories from Macintosh workstations.
3. If appropriate, enable the Windows File Server. If Windows file services are not enabled, users will not have access to their personal network directories or shared team directories from Windows workstations.
4. If you enable the Windows File Server, enter a Windows workgroup name. This name indicates the workgroup under which Net Integrator will be listed as a resource in Windows Network Neighbourhood.
Please Note: It is recommended that you enter the Windows workgroup name being used by other workstations in the office. If you are setting up a new network, you can use any workgroup name you wish – just make sure that you configure your Windows workstations so they belong to the same workgroup.
5. If appropriate, enable the domain controller. The Windows File Server will then act as the Windows domain controller. The Windows workgroup name will then become your network Domain Name.
Please Note: The Windows File Server must be enabled for the domain controller to function. See *Chapter 7: Domain Controller* for more information.
Please Note: Your network domain name has nothing to do with your internet domain name. They do not interact and are independent of each other.
Advice/Recommendation: Do not use the same internet domain name as your local network domain name.
6. Enter an administrative password for the domain controller. This will be used to add workstations to the domain. Re-enter the password to ensure it was entered correctly.
7. If appropriate, enable the NFS File Server. If NFS file services are not enabled, UNIX users will not have access to their personal network directories or shared team directories from UNIX workstations.
8. Click on the *Save Changes* button.
9. To ensure that the status of the file server has changed, select *System Status* from the menu on the left hand side of the screen. The *Windows*, *Apple*, and *NFS File Server* sections of the *System Status* screen display the updated status.
Please Note: It may take up to 15 seconds for file services to start, and during that time the status may read *Error starting service*.

What is a Domain Controller?

A domain controller provides authentication services to the rest of the computers on the network. It stores user account and security information in a central database for one domain. When a user logs on to a computer that is part of the domain, the domain controller authenticates the username and password against the information in the directory database.

Net Integrator can serve as a Windows domain controller for all the computers running Windows on the network. When this function is enabled, the Windows file server is set up as a domain controller and a domain name will replace the Windows workgroup.

Please Note: The Windows file server must be enabled for the domain controller to function.

Please Note: Your network domain name has nothing to do with your internet domain name. They do not interact and are independent of each other.

Advice/Recommendation: Do not use the same internet domain name as your local network domain name.

Configuring the Domain Controller

To enable Net Integrator's domain controller function:

1. Select *File* under *Server Setup* from the menu on the left side of any WebConfig screen. The *File Server Setup* screen displays:

FILE SERVER SETUP		
Enable File Virus Scanner?	☒ Yes ☐ No	?
Enable Macintosh file server?	☐ Yes ☒ No	?
Enable Windows file server?	☒ Yes ☐ No	?
Windows workgroup name:	WORKGROUP	?
Enable Domain Controller for Windows?	☒ Yes ☐ No	?
Domain Controller: Enable roaming profiles?	☐ Yes ☒ No	?
Domain Controller: Admin password (username is _root):		?
Domain Controller: Re-enter admin password:		
Enable NFS file server?	☐ Yes ☒ No	?
Mapping scheme for NFS:	☒ upadd ☐ Mmap	?

☒ SAVE CHANGES
 ☐ FILE SYNC..
 ☒ CANCEL CHANGES

2. Ensure that the Windows file server is enabled.
3. Enter a name in the *Windows workgroup name* field. This will be the domain name once the domain controller is enabled. Avoid using the default name of “Workgroup”, as it could be very confusing.
Please Note: You will need to set each Windows workstation's domain name to match this, in order for Windows file and printer sharing to work properly.
4. Enable the domain controller for Windows.
5. Enter the administrative password for joining computers to the domain. Re-enter the password to ensure it was entered correctly.
6. Click on the *Save Changes* button.

Joining Windows Systems to a Domain

All Windows workstations will have to be added to the domain once the domain controller is enabled. The predefined administrative username needed to add a system to the domain is always *_root*.

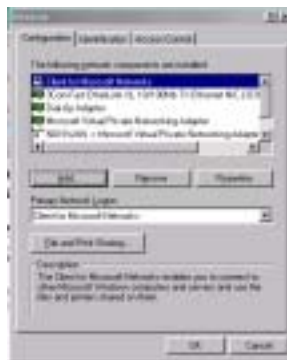
For Windows 95/98/ME:

A Windows 95/98/ME workstation does not actually join the domain. However, it is able to log onto the domain with the following steps:

1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* window displays:



2. Select *Network* from the list. The *Network* window displays. Click on the *Configuration* tab.



-
- Share for Microsoft Exchange Properties**
- General**
- Logon location**
- ☒ Log on to Windows NT domain
- When logging on, use a password that is valid on a Windows NT domain.
- Log on to Windows NT domain
-
- Network logon options**
- ☐ Quick logon
- Windows log on only into the network, but network drive access is suspended until you are done.
- ☒ Log on and restore network connections
- When logging on to the network, Windows restores that each network drive is ready to use.
- OK Cancel**

- For Windows NT:*

-

2. Select *Network* from the list. The *Network* window displays. Click on the *Identification* tab.



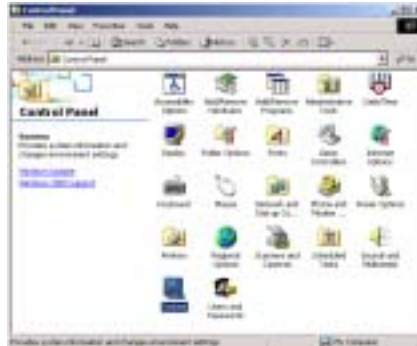
3. Click on the *Change* button. The *Identification Changes* window displays:



4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup WebConfig* screen).
5. Check the box for *Create a Computer Account in the Domain*. Enter the administrative username, *_root*, and the password (as entered in the *Domain Controller Password* field on the *File Server Setup WebConfig* screen).
6. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
7. Reboot the workstation. The next time you log on, the login window will have an additional *Domain* field.

For Windows 2000:

1. In Windows, select *Start > Settings > Control Panel*. The *Control Panel* displays:



2. Select *System* from the list. The *System Properties* window displays. Click on the *Network Identification* tab.





4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

For Windows XP Professional:

1. Install the registry patch: http://www.net-itech.com/america/support/registry_patch/samba_xp_domain_member.reg

For information on the latest features available in Samba as a domain controller, download this PDF: <http://www.net-itech.com/america/support/docs/csamba6.pdf>

2. In Windows, select *Start > Control Panel*. The *Control Panel* window displays. On the left menu bar under *Control Panel*, select *Classic View* if you are currently in *Category View*.



3. Select *System* from the list. The *System Properties* window displays. Click on the *Computer Name* tab.



4. Click on the *Change...* button. The *Computer Name Changes* window displays:



5. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup WebConfig* screen).
6. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

File Mounting/Drive Mapping

Once the domain controller is enabled, a user's files can be mounted directly onto any domain workstation upon login. The shared files of any team that the user belongs to can also be mounted.

For Users:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. Click on the *Edit Action* button for the appropriate user. The *Modify User* screen displays:

MODIFY USER	
User ID:	anyuser
Full Name:	Any Old User
Password:	
Re-enter Password:	
Administrator Access:	☐ Yes ☐ No
Allow FTP Access:	☐ Yes ☐ No
Allow YTS (FTP) and Dial-In Access:	☐ Yes ☐ No
Allow in Exchange Mail System:	☐ Yes ☐ No
Automatically mount files as:	C:
Join Teams:	☐ /boardroom ☐ /exchange-admin ☐ /eng ☐ /marketing ☐ /staff ☐ /support
Test E-Mail:	Test

2. From the drop-down menu in the *Automatically mount files as* field, select the drive that the user's files should be mounted as on the workstation. The default drive is X:.
Please Note: Be sure to choose a drive that will not conflict with drives already in use.
3. Click on the *Save Changes* button.

This can also be done when the user is created.

For Teams:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. Click on the *Edit Action* button for the appropriate user. The *Modify Team* screen displays:

The screenshot shows the 'MODIFY TEAM' web interface. It has a blue header with the title 'MODIFY TEAM'. Below the header are several form fields: 'Team ID' (ftp), 'Full Name' (Anonymous FTP Admin), 'Password' (empty), and 'Set new Password' (empty). There are two radio buttons for 'Allow FTP Access' (selected) and 'Allow FTP (FTTP) and Shell Access' (selected). Below these are radio buttons for 'Group Email' (Selected to send email, Use shared folder, Not to send any). A dropdown menu for 'Automatically mount files as' is set to 'None'. Below the form are four buttons: 'CONVERT TO USER', 'E-MAIL...', 'SAVE CHANGES', and 'CANCEL CHANGES'.

2. From the drop-down menu in the *Automatically mount files as* field, select the drive that the team's shared files should be mounted as on the workstation. The default, *None*, is to not mount the files at all. This ensures that there will be no conflict between use of drive space.
3. Click on the *Save Changes* button.

This can also be done when the team is created.

Logon Scripts

Logon scripts are supported through DOS batch files found at \\Servername\netlogon. All scripts are called "username.bat". These batch files will call upon "logon.bat". If manual modifications are required - create the file called "logon.bat" All manual modifications should be made to "logon.bat" as "username.bat" is automatically generated, and modifications will be lost!

Automated Drive Mapping

User folders and team folders can be automatically mounted through the selection of a drive mount in the User/Team setup. These drive mappings are done through the Logon scripts. Note that any drives previously mounted will not be automatically disconnected as Windows caches these drive connections.

Net Integrator Print Services

Net Integrator's parallel printer port can be connected to any type of printer that users are sharing on the internal network. Net Integrator does not support the bidirectional mode of parallel devices; it can send output to printers but cannot read detailed status information. This means that any special print manager and status monitor software on your PC should be disabled. Net Integrator's print services are setup automatically during the first system boot (providing all Net Integrator users with unrestricted access to the shared printer).

The administrator/installer is required to provide the appropriate drivers for the specified printer at the workstation.

Please Note: Only parallel port printers are supported. Print Services does not support USB printers or "green" enabled printers that shut themselves off when there is inactivity on the port.

Configuring Print Services

Before you can print on a printer connected to your Net Integrator, you have to configure your Net Integrator for printing.

1. Click on the *Printers* button on the WebConfig screen. Net Integrator will list all the available printers.



2. Choose to enable Print Services or not. Without this option being set you will not be able to print using the printers attached to this server.
3. Click the *Save Changes* button.

Configuring your Workstation

1. In Windows, open your Network Neighbourhood and double-click on the server icon with the name of your Net Integrator (e.g. *Paintball*). The following window shows the network file and print services to which you have access:



2. Double-click on the printer icon. The following window displays:



3. Select *Yes* to configure your workstation. The *Add Printer Wizard* displays:



4. Select *No* to indicate that you are not printing from MS-DOS programs. Click on *Next*.

5. Select the brand and type of printer that is connected to your Net Integrator. Click *Next*.

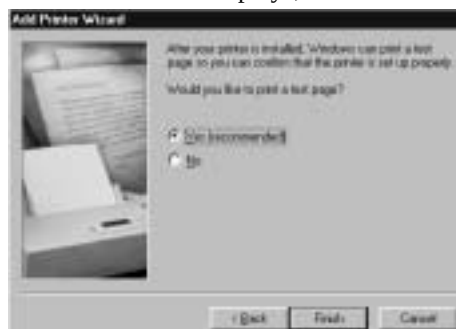


Please Note: If your printer is not listed, click on the *Have Disk* button and provide the printer driver from the disk provided by your printer's manufacturer.

6. Enter a name for the printer. Indicate whether or not you want this printer to be used as the default printer. Click on the *Next* button.



7. On the screen that displays, indicate whether or not you want to print a test page.



8. Select Finish. You will be prompted to insert your Win95/98 install disk. Some files will be copied to your system, and your shared printer will be setup and ready for printing.

Components of the Email System

The main components of Net Integrator's email delivery subsystem are the:

- **SMTP Server** – a mail delivery system. When you send an email, the SMTP server takes this message from your email client and delivers the message to the recipient's POP3 server. If your ISP forces you to use a specific SMTP server, the Net Integrator can deliver to that server rather than directly to the destination servers. This is known as a "smarthost".
- **POP3 Server** – a system that receives a user's email messages and stores them in the user's mailbox. When a user's email client checks for new mail, it communicates with the POP3 server, which ensures proper user authentication and delivery of email to the user's email client. POP3 is the most commonly used mail delivery protocol.
- **POP3/SSL Server** – this is the secure POP3 server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **IMAP Server** – an advanced system that is similar to POP3. Because IMAP is relatively new, not all mail clients support it. IMAP offers superior user authentication and allows users to store their email on a server instead of downloading messages to a workstation (as is the case with POP3). This allows users to check their email from various workstations and lets them see a complete list of the emails kept in their folders.
- **IMAP/SSL Server** – this is the secure IMAP server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **WebMail Server** – a system that allows users to securely access their email from any workstation on the Internet using a standard web browser. The web mail server uses SSL encryption to secure online transactions. Refer to *Chapter 10: WebMail* for more information.
- **LDAP Server** – a directory system that holds the names and email addresses of all users on the Net Integrator server. This directory can be searched with any standard email client. The LDAP server does not store names and email addresses of users not connected to the Net Integrator.

- **Real-time Blackhole List (RBL)** – a ‘spam’ blocker that has different levels of spam protection (*Strong* and *Medium*).
- **Mail Virus Scanner** – scans all outgoing and incoming mail for viruses. If a virus is found, it is immediately removed from the email. A warning is then sent to the sender and all recipients along with the original (but virus-free) message. You must buy the license for your Net Integrator for this feature to be enabled.

Configuring Email Service

1. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays:

E-MAIL SETUP		
SMTP (out delivery) server:	☒ Yes ☐ Only Trusted Hosts ☐ No	?
POP3 (out delivery) server:	☒ Yes ☐ Only Trusted Hosts ☐ No	?
POP3 SSL (secure out delivery) server:	☒ Yes ☐ Only Trusted Hosts ☐ No	?
IMAP (advanced mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No	?
IMAP SSL (secure advanced mail reader) server:	☒ Yes ☐ Only Trusted Hosts ☐ No	?
Web Mail Server (Requires IMAP, MySQL and secure WWW servers)	☒ Yes ☐ No	?
Exchange/IT Server (Requires MySQL and secure WWW servers)	☒ Yes ☐ No	?
LDAP directory server:	☒ Yes ☐ No	?
RBL (outgoing blackhole)	☒ Strong RBL ☐ Medium RBL ☐ No RBL	?
Mail Virus Scanner:	☒ Yes ☐ No	?
Minutes between remote POP mailboxes checks:	5	?
Mail Domain:	abc.com	?
ISP's SMTP Server:		?

☒ SAVE CHANGES
 ☒ EMAIL ALIASES
 ☒ CANCEL CHANGES

2. Select the appropriate SMTP server setting:
 - Selecting *Yes* enables the SMTP server and allows any computer on the internal network or on the Internet to send email using the Net Integrator as a mail server. Messages from computers on the Internet are accepted only if their destination is the local domain hosted by your Net Integrator. (This prevents your server and Internet bandwidth from being used to send unsolicited emails).

- Selecting *Only Trusted Hosts* enables the SMTP server and allows internal users and users connected to the internal network through a VPN to send email using the Net Integrator as their mail server.
 - Selecting *No* disables the SMTP server completely.
3. Select the appropriate POP3 server setting:
 - Selecting *Yes* enables the POP3 server and allows any computer on the internal network or on the Internet to access the POP3 mailbox. Select *Yes* only if you have users who will be accessing their email from outside of the office.
 - Selecting *Only Trusted Hosts* enables the POP3 server and allows internal users to access the POP3 mailbox.
 - Selecting *No* disables the POP3 server completely.
 4. Select the appropriate POP3/SSL server setting
 - Selecting *Yes* will allow incoming secure POP-3 connections from anywhere. This means that your users could download their email from anywhere on the Internet.
 - Select *Only Trusted Hosts* to allow incoming secure POP-3 connections only from the local network, and not from the Internet.
 - Select *No* to disable the secure POP-3 server.
 5. Select the appropriate IMAP/SSL server setting
 - Selecting *Yes* will allow incoming secure IMAP connections from anywhere. This means that your users could read their E-Mail from anywhere on the Internet.
 - Select *Only Trusted Hosts* to allow incoming secure IMAP connections only from the local network, and not from the Internet.
 - Select *No* to disable the secure IMAP server.
 6. Select the appropriate IMAP server setting:
 - Selecting *Yes* enables the IMAP server and allows any computer on the internal network or on the Internet to access the IMAP mailbox. Select *Yes* only if you have users who will be accessing their email from outside of the office.
 - Selecting *Only Trusted Hosts* enables the IMAP server and allows internal users to access the IMAP mailbox.
 - Selecting *No* disables the IMAP server completely.
 7. Select the appropriate WebMail server setting:
 - Selecting *Yes* enables the WebMail server. Enabling the WebMail server automatically enables the IMAP and WWW servers. If you disable IMAP or the WWW servers, the WebMail server will not be functional.
 - Selecting *No* disables the WebMail server completely.

8. Select the appropriate LDAP directory server setting:
 - Selecting *Yes* enables the LDAP server (which answers directory queries). The LDAP directory is automatically populated with the names and email addresses of all users configured on the Net Integrator server.
 - Selecting *No* disables the LDAP server completely.
9. Select the appropriate RBL setting:
 - Select *Strong RBL* if you want to block known spam servers and spam relay servers. Strong RBL blocks all spam mail, but may also block other mail. Senders receive a message if their mail is blocked.
 - Select *Medium RBL* if you want to block known spam servers. Medium RBL blocks most spam mail.
 - Select *No RBL* if you do not want spam protection.
10. Indicate whether or not you want to enable the Mail Virus Scanner. By default, the virus scanner is enabled.
11. Enter the number of minutes between remote POP mailbox checks. The number in this field specifies how often (in minutes) the remote mailbox is checked for new emails.
12. Enter the name of your mail domain (e.g. `example.com`).
13. In the field for *ISP's SMTP Server* enter the server name if your ISP forces you to use a specific SMTP server. This will make the Net Integrator deliver to that server rather than directly to the destination servers. This is known as a “smarthost”. You should leave this blank whenever possible.
14. Click on the *Save Changes* button.

Clearing the Email Queue

Clear Email Queue allows you to clear the outgoing email queue.

1. Select *Email* from the menu on the left side of any WebConfig screen. The *Email Setup* screen displays

2. Click on the *Clear Email Queue* button. The *Clear email queue?* prompt displays:

Clear email queue?

Are you sure you wish to clear your email queue?



3. Click on *Yes* to clear the email queue. You will be brought back to the *Email Setup* screen.

Configuring Email Aliases

The Email Alias feature allows you to assign an email address that is used for redirection of the incoming email to one or more recipients. The incoming mail may also be redirected to external email addresses.

Create Email Alias Account:

1. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays.

2. Click on the *Email Aliases* button. The *Email Aliases* screen displays:

EMAIL ALIASES		
Alias Name	Target Name	Action
abuse	postmaster	 
MAILER-DAEMON	root	 
postmaster	root	 

 [ADD ALIAS](#)

 [HOME](#)

3. Click on the *Add Alias* button. The *New Email Alias* screen displays:

NEW EMAIL ALIAS		
Alias name:		
Target name(s):		

 [SAVE CHANGES](#)

 [CANCEL CHANGES](#)

4. Enter the alias email address in the *Alias name:* box. An email that is sent to an email alias will be sent to the target(s) that you specify. For example, if you want the email alias of sales@domain.com, you would enter the alias name “sales”.
5. In the *Target name(s):* box enter the alias’ mail box(es) to whom an email will be forwarded when it is directed to the alias name .

Please Note: The target field can either be a mail box on the same domain (for example 'root') or an external e-mail address (such as 'user@otherdomain.com') or a forward reference to another alias. If there is more than one target, they can be separated by commas or spaces. A target name may not contain any other non-alpha-numeric characters. If it does, the invalid characters will be replaced by "_". All characters will be converted to lower case if they are not already so.

- Click on the *Save Changes* button. The *Email Aliases Notices* screen displays notifying you that it is *Adding alias name 'aliasname'*:

NOTICES		
	Adding alias name 'aliasname'.	

EMAIL ALIASES		
Alias Name	Target Name	Action
aliasname	anyperson@abc.com	
MAILER-DAEMON	root	
postmaster	root	

ADD ALIAS **HOME**

- Click on the *Add Alias* button to add another alias or click on the *Home* button to return to the *Email Aliases* screen. The new alias name displays in the list of previously created aliases.

Edit/Delete Aliases

To edit an Email Alias:

- On the *Email Aliases* screen, click on the appropriate alias' *Edit Action* button:

EMAIL ALIASES		
Alias Name	Target Name	Action
aliasname	anyperson@abc.com	
MAILER-DAEMON	root	
postmaster	root	

ADD ALIAS **HOME**

- The *Modify Email Alias* screen displays:

- Change the alias' information as appropriate.
- Click on the *Saves Changes* button.

To delete an Email Alias:

- On the *Email Aliases* screen, click on the appropriate alias' *Edit Action* button. The system will prompt you with *Are you sure you want to delete aliasname?* Click *OK*.

- The *Email Aliases Notices* screen displays notifying you that it is *Deleting alias 'alias-name'*. Click on the *Add Alias* button to add another alias, click on the appropriate alias' *Edit Action* button to delete another alias, or click on the *Home* button to return to the Email Aliases screen.
- Click on the *Saves Changes* button.

Configuring DNS Records

Although email services are fully functional after the administrator enables the appropriate mail servers, the mail delivery DNS records have to be configured before users can send mail to and receive mail from outside users.

How do DNS Mail Records work?

When you send an email to `johndoe@example.com`, the message is downloaded to your SMTP server (which needs to know the IP address of `example.com` in order to deliver the message). The SMTP server consults the root DNS server on the Internet and through a series of queries is eventually pointed to the DNS server that stores the names and IP numbers of the hosts in `example.com`.

DNS Resolution

It is vital that your DNS server (which maintains information about your domain) is set up correctly. DNS resolution service can be provided by Net Integrator, or it can be provided by another DNS server maintained by you or by your ISP. If DNS resolution is provided by your ISP and you want Net Integrator to receive all emails for your domain, then make sure that you request the following from your ISP:

MX records for your domain should be pointed to your Net Integrator's outside IP address (the address assigned to the eth1 interface).

If DNS resolution is provided by Net Integrator, make sure that the outside IP address is registered with Network Solutions as your domain DNS host.

Please Note: In order for your Net Integrator to function properly as a mail server for global email delivery, you must have a static IP address or use Dynamic DNS.

Configuring Net Integrator as a DNS Server

1. Selecting *Local* from the *Network Setup* menu on the left side of any WebConfig screen. The *Local Network Options* screen displays:

The screenshot shows the 'LOCAL NETWORK OPTIONS' screen in the Net Integrator web interface. On the left is a navigation menu with categories like SYSTEM STATUS, LOGIN SETUP, SOFTWARE UPDATE, LOGS/REPORTS, TASK SCHEDULE, SERVER SETUP, FILE, E-MAIL, WWW, FTP, DNS, and BACKUP. The 'LOCAL' option under NETWORK SETUP is selected. The main panel contains several configuration fields:

- Host Name: 192.168.1.100
- Domain Name: 192.168.1.100
- Enable proxy server? [Yes] [Only Trained Users] [No]
- Act as public DNS server? [Yes] [No] [Dynamic]
- Run DHCP server on: [v] [v] [v] [v]
- Enable DHCP server (read only)? [Yes] [No]
- DHCP reservation name: 192.168.1.100
- Enable Active Queue Management? [Yes] [No]
- Enable NAT server? [Yes] [No]
- Enable outgoing connections? [Yes] [No]
- System Time (Show Internet): Fri May 12 11:41:13 2005
- Adjust Time Zone: GMT-8

At the bottom, there are buttons for 'SAVE CHANGES' and 'CANCEL CHANGES', and a link for 'ADVANCED'.

2. In the *Act as public DNS server* field, select *Yes*.
3. Click on the *Save Changes* button.

Configuring Email Clients

Although there are a number of different email clients available today, the configuration of most email clients is very similar. The exact configuration of your email client depends on how you want your mail delivery to be configured. The two most common configurations are listed below. Configure your mail client according to the configuration that resembles your email setup.

1. **If your mail is hosted on your ISP's mail server...**

All users in your office have their own mail address and mailbox hosted on the ISP's server. Your ISP supplies you with the name of the POP3 or IMAP server where your mail has to be retrieved and with the address for the SMTP mail delivery server. Enter this address into the appropriate field during the configuration of your mail client.

Using your Net Integrator as an SMTP server (even if your mail is hosted by an ISP) has its advantages, especially if you often send large messages or if you have a slow Internet connection. Your email client may be tied up for minutes or even hours if you attempt to send a large email message to an ISP's SMTP server. If you use your Net Integrator as an SMTP server, large files are quickly transferred over the high-speed LAN. Although a file is then slowly transferred over your Internet connection, your email client is free to perform other tasks.

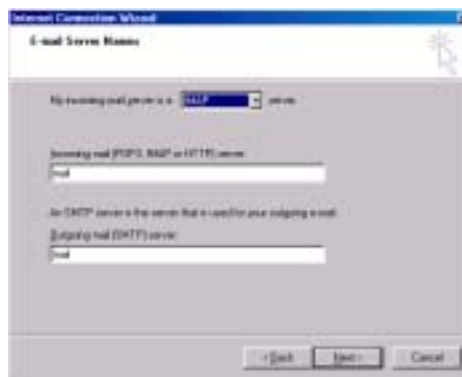
Enter the following information when configuring your email client:

- In the *SMTP server* field, enter the IP address or host name provided to you by your ISP. Alternatively, use your Net Integrator as the SMTP server and enter the IP address or host name of your Net Integrator.
- In the *POP3* or *IMAP server* field, enter the IP address or host name provided to you by your ISP.
- In the *POP3* or *IMAP mailbox name* field, enter the first part of your email address. For example, if your email address is johndoe@example.com, enter johndoe into this field.
- In the *POP3* or *IMAP password* field, enter the password provided to you by your ISP.

2. If your mail is hosted on Net Integrator...

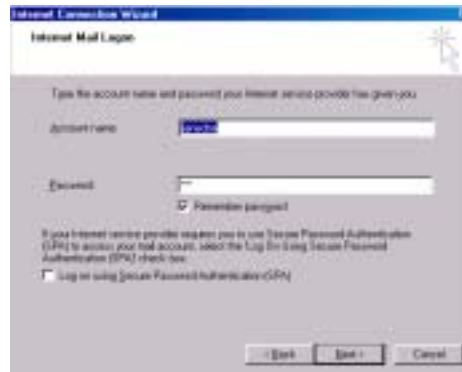
Enter the following information when configuring your email client:

- In the *SMTP server* field, enter the IP address or host name of your Net Integrator. You do not need to enter the domain name.
- In the *POP3* or *IMAP server* field, enter the IP address or host name of your Net Integrator.



- In the *POP3* or *IMAP mailbox name* field, enter your Net Integrator username.

- In the *POP3* or *IMAP* password field, enter your Net Integrator password.



Advanced Email Settings

The following are advanced features of Net Integrator's email system:

- **POP Retriever** – Net Integrator can automatically retrieve emails from a remote mail account and store them in a user's local mailbox. This means that instead of checking two accounts for new email, users can simply check their local Net Integrator account.

This has some advantages for the user, particularly for emails with large attachments. Normally, users have to configure their mail clients to receive mail from a local account and a remote account. With this dual-mail box approach, receiving emails with large file attachments from remote email accounts can be quite slow (depending on the available Internet bandwidth). The POP Retriever improves the speed considerably because it 'pre-retrieves' emails.

- **Mail Forwarding** – Net Integrator can automatically forward mail that has been received from a remote mail account to a user's local mailbox.
- **Auto Reply** – Net Integrator can automatically send a reply message to every email received by a user.

Please Note: To modify user's advanced email settings, refer to *Modifying User Email Settings* in *Chapter 5: User & Team Management*.

LDAP Server

Net Integrator has a built-in Lightweight Directory Access Protocol (LDAP) server, which provides a directory of user names and email addresses. It is automatically populated with names and email addresses of all Net Integrator users. Most email clients support access to read-only LDAP servers.

Configuring LDAP in Microsoft Outlook

1. Open Microsoft Outlook. From the main menu, select *Tools > Accounts*. The *Internet Accounts* screen displays:

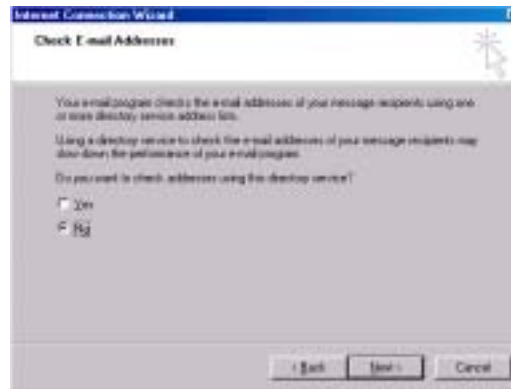


2. Select *Add > Directory Service*. The *Internet Connection Wizard* displays:

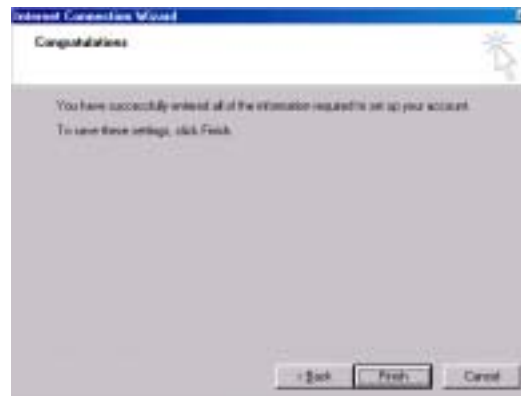


3. In the *Internet directory (LDAP) server* field, enter the name **or** IP address of your Net Integrator.

4. Click on the *Next* button. The following screen displays:



5. Indicate whether or not you want your email client to check addresses using the LDAP directory.
Please Note: If this option is selected, you can enter partial email addresses when sending emails. Outlook will automatically find the closest match in the LDAP directory and enter the correct email address.
6. Click on the *Next* button. The following screen displays:



7. Click on the *Finish* button. The *Internet Accounts* screen re-displays. Click on the *Properties* button. Select the *Advanced* tab on the screen that displays.

8. The *Advanced* screen displays:



9. In the *Search Base* field, enter *o=example.com*.
Please Note: Replace *example.com* with the Internet domain hosted by your Net Integrator.
10. Click on the *OK* button. The *Internet Accounts* screen re-displays. Click on the *Close* button. The LDAP server is now set-up, and users can search through the LDAP data directory for the names and email addresses of Net Integrator users.

WebMail Server

Net Integrator's WebMail server allows you to access your email using a standard web browser from any workstation connected to the Internet. Your communications are kept secure with SSL encryption.

Please refer to the *Net Integrator WebMail Usage Guide* for specific functionalities not covered in this manual.

Enabling WebMail Server

The WWW-based WebMail email server uses IMAP and a secure encrypted WWW connection; therefore, the Secure WWW Server and IMAP server must be enabled in WebConfig in order for WebMail to become available.

When enabled, Web Mail can be reached at: <https://yourservername.com/email>.

Please Note: For users to access WebMail from elsewhere on the Internet, the Secure WWW Server must be set to allow connections from anywhere, but the IMAP server can be set to accept connections from Only Trusted Hosts. (It is the WWW server on the local network that establishes the IMAP connection).

1. To enable the server configurations for WebMail, log in to WebConfig.

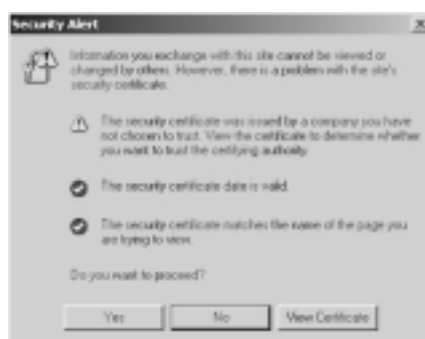
2. Select *E-Mail* from the *Server Setup* menu found on the left side of any WebConfig screen. The *E-Mail Setup* screen displays:

3. Select *Yes* in the *Web Mail Server (Requires IMAP, MySQL and secure WWW servers)* box.
4. Click on *Save Changes*.
5. Select *WWW* from the *Server Setup* menu found on the left side of any WebConfig screen. The *WWW Setup* screen displays:

6. Select *Yes* in the *Enable WWW server?* box.
7. Select *Yes* in the *Enable secure WWW server?* box.
8. Select *Yes* in the *Enable MySQL Server?* box.
9. Click on *Save Changes*.

Accessing WebMail

1. Open a web browser from any workstation that is connected to the Internet.
2. Enter the address of your Net Integrator into the browser's address bar.
 - If your Net Integrator provides DNS resolution for your domain, enter information in the following format:
`http://server.domain.com/email`. For example, if your server name is *alpha* and your domain name is *example.com*, enter
`http://alpha.example.com/email`. You can also enter information in the following format: `http://www.example.com/email`.
 - If your Net Integrator does not provide DNS resolution, enter your Net Integrator's external IP address. To find the external IP address, select *Local* from the *Network Setup* menu. On the screen that displays, click on the *Advanced...* button. In the *Network Devices* section of the screen that displays, look at the IP address of the *eth1* interface. If the address is *204.1.30.12*, enter
`http://204.1.30.12/email`.
3. What happens next depends on how your web security certificate was generated. If your security certificate was generated by Net Integrator (and not assigned to you by a certificate authority), the following security alert may display when you login to WebMail:



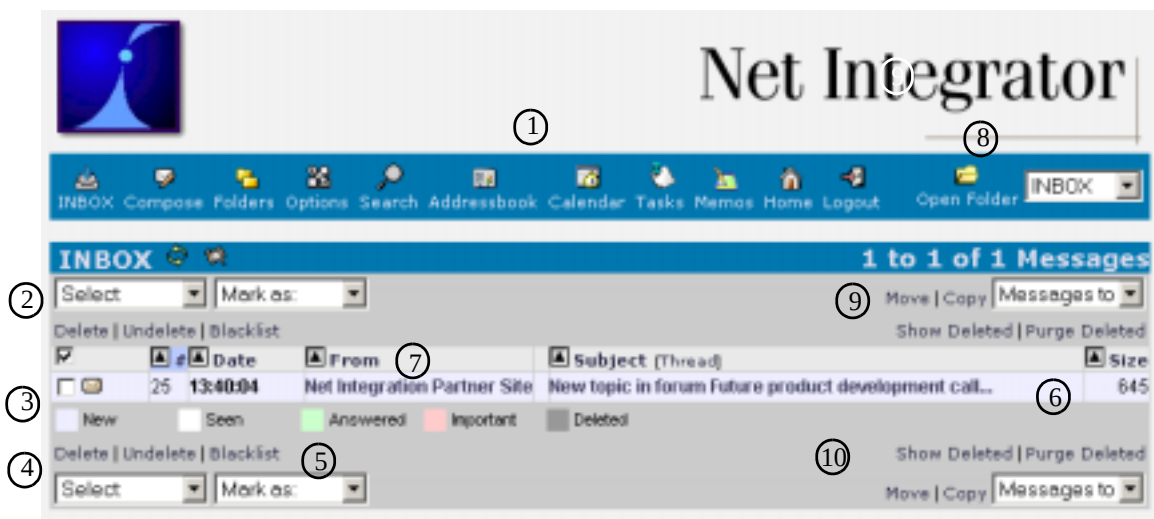
Please Note: This alerts the user that the security certificate presented by Net Integrator cannot be verified for authenticity. If you want a certificate that is authenticated by a certificate authority, you will have to purchase one. Please refer to *Chapter 11: Web Services* for more information.

- Click on the Yes button to continue. The following screen displays:



- Enter the username and password that you use to login to Net Integrator. Click on the *Login* button. The *WebMail* screen displays.

Using the WebMail Screen



- From the *Main Webmail Menu*, click on the:
 - Inbox* button to view the contents of your inbox.
 - Compose* button to compose a new email message. See *Composing an Email Message* for more information.

-
- *Folders* button to view a screen that lists your folders. On this screen, you can create, edit, and delete folders.
 - *Options* button to view a screen that lists various configuration options. See *Configuring WebMail* for more information.
 - *Search* button to search for a specific message. Refer to *Search Function* for more information.
 - *Addressbook* to view your address book. On this screen you can add, edit, and delete address entries. See *AddressBook* for more information.
 - *Calendar* to view your personal calendar. See *Calendar* for more information.
 - *Tasks* to view your list of tasks. See *Tasks* for more information.
 - *Memos* to view your memos. See *Memos* for more information.
 - *Home* to return to the *Main Webmail Menu*.
 - *Logout* button to log out of WebMail.
2. To give a message a specific status (such as *seen* or *unseen*), select an option from the *Select* list or place a check in a message's checkbox and select an option from the *Mark as* list.
 3. Place a check in the *Message Checkbox* to select one or more messages.
 4. To delete or undelete a message, place a check in its message checkbox and then click on the *Delete* or *Undelete* button.
 5. To block messages from a specific person, place a check in the message's checkbox and click on the *Blacklist* button. See *Mail Filters* for more information.
 6. The *Message List* displays information pertaining to received messages. Click on a link in the *From* or *Subject* section of the screen to open a message.
 7. To sort the messages in your inbox, click on the *Date*, *From*, *Subject*, or *Size* message headings.
 8. To open a folder, select it from the list and click on the *Open Folder* button.
 9. To move or copy a message to another folder, place a check in its message checkbox and then click on the *Move* or *Copy* button.
 10. To move a message to your trash folder, place a check in its message checkbox and then click on the *Hide Deleted* button. You can show them again by clicking on the *Show Deleted* button. To empty the contents of the trash folder, click on the *Purge Deleted* button.

Configuring WebMail

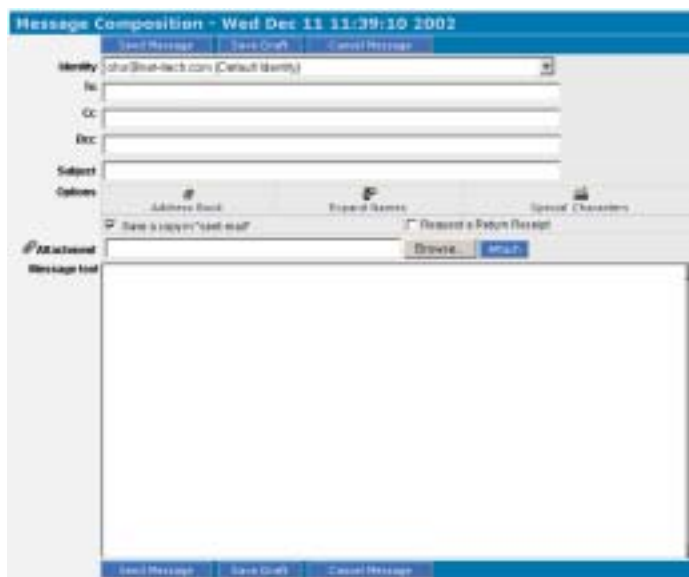
1. From the *Main WebMail Menu*, click on the *Options* button. The *Options* screen displays:



2. Click on any of the headings (such as *Personal Information*, *Filters*, and *Display Options*) to change your WebMail settings.
3. Follow the instructions on the screen that displays.
4. Click on the *Save Options* button to save your changes and return to the *Options* screen.

Composing an Email Message

1. From the *Main WebMail Menu*, click on the *Compose* button. The *Compose* screen displays:



2. Enter the email address of the recipient(s) in the *To* field. If the recipient is in your address book, you can enter a partial name (e.g. *john* instead of *john.doe@example.com*).
3. Enter the email address(es) of those you wish to receive a copy of this email in the *Cc* (*Carbon Copy*) field.
4. If you want to send someone a copy of this email without the knowledge of the other recipients, enter their email address in the *Bcc* (*Blind Carbon Copy*) field.
5. Enter the subject of the email in the *Subject* field.
6. If you entered a partial name in the *To* field, you can click on the *Expand Names* button to view the recipient's full name and email address.
7. To insert any special characters into your message, click on the *Special Characters* button. On the screen that displays, select a character from the appropriate list and paste it into your message.
8. If you do not want a copy of this email saved in your *Sent-Mail* folder, remove the check from the box.

9. Place a check in the *Request a Return Receipt* box if you want the recipient to notify you when they receive your message.

Please Note: The recipient can choose not to send a return receipt to you.

10. To attach a document to your message:

- Click on the *Browse...* button.
- Select the file from the window that displays and click on the *OK* button. The file displays in the *Attachments* field.
- Click on the *Attach* button.

Please Note: To remove an attachment, place a check in the attachment's checkbox and click on *Remove Selected*.

11. Enter the message content in the empty section of the screen.
12. Click on the *Save Draft* button if you want to save this message in your *Drafts* folder. Click on the *Send* button to send the message to the recipient(s).

Please Note: Clicking on the *Cancel* button prior to sending the email aborts the message.

Opening a Received Message

1. From your inbox, click on a link in the *From* or *Subject* section of the screen. The message opens:



2. You have many options after reading the message. Click on:
 - *Delete* to send this message to your trash folder.
 - *Reply* to send a reply to the person that sent you the message.
 - *Reply to all* to send a reply to everyone who received the message.
 - *Forward* to forward this message to another recipient.

- *Redirect* to send this message directly to another recipient (without the opportunity to add comments).
 - *Blacklist* to create a rule that sends mail from this person to your trash folder instead of your inbox. See *Mail Filters* for more information.
 - *Message Source* to open a window that displays information about this email.
 - *Print* to print this message. The message displays in another window and a Print window appears. Click on *OK* to print your message.
3. To move or copy this message to another folder, select the appropriate folder from the drop-down list and click on the *Move* or *Copy* button.
 4. Click on *Back to Inbox* to return to your inbox.

Replying to a Message

1. After opening and reading a message, click on *Reply* or *Reply to all*. Your choice depends on the intended recipient(s).
2. The *Reply* screen displays.
Please Note: The *Reply* screen is the same as the *Message Composition* screen, except that the previous correspondence displays. Refer to *Composing an Email Message* (in this chapter) for information about this screen.
3. Enter your reply.
4. Click on the *Save Draft* button if you want to save this message in your *Drafts* folder. Click on the *Send* button to send the message to the recipient.
Please Note: Clicking on the *Cancel* button prior to sending the email aborts the message.

Search Function

WebMail's *Search* function allows you to search for a message or set of messages using specific criteria:

1. From the *Main WebMail Menu*, click on the *Search* button. The *Search* screen displays:

2. Enter information into the appropriate *Message fields*.
3. Select the appropriate *Message flags*.
4. Select the appropriate *Message folders*.
5. Click on the *Search* button to begin the search.
Please Note: Click on the *Reset* button prior to clicking on the *Search* button to clear your search criteria.
6. The *Search Results* screen displays, showing all of the messages that match your search criteria. If no messages display, you can perform another search using different criteria.

Address Book

Adding an Entry

1. From the *Main WebMail Menu*, click on *Addressbook*. The following screen displays:

Name	Email
John Doe	john.doe@example.com

2. Click on the *Add* button. The *Add New Contact* screen displays.
3. Enter all appropriate information and click on the *Save* button.

Performing a Directory Search

1. Click on the *Search* button. The *Directory Search* screen displays.
2. Select *Name* or *Email* from the *Find* drop-down list.
3. Enter the search criteria and click on the *Search* button. The results display in the *Search Results* section of the screen.
Please Note: Clicking on the *Search* button without search criteria returns all of the addresses in your address book.
4. To perform an advanced search:
 - Click on the *Advanced Search* button. The *Advanced Directory Search* screen displays.
 - Enter appropriate search criteria and click on the *Search* button.
 - The results display in the *Search Results* section of the screen.
5. To send a message to this person, place a check in the checkbox beside their name and click on the *Send Message* button. To clear the *Search Results* section of the screen, click on the *Clear Search* button.

Importing and Exporting Addresses

1. To import addresses from another source:
 - Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Import Addressbook* section of the screen, select the format to export from (your options are *CSV*, *Outlook CSV*, and *vCard*).
 - Select the destination (should be *My Addressbook*).
 - Select the file to import. Either enter the file name directly into the empty field or select it by clicking in the *Browse...* button.
 - Click on the *Import* button.
2. To export addresses to another source:
 - Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Export Addressbook* section of the screen, select the format to export to.
 - Select the source to export from (should be *My Addressbook*).

- Click on the *Export* button.
- Select a location for the file and click on the *OK* button.

Calendar

1. From the *Main WebMail Menu*, click on the *Calendar* button. The WebMail calendar displays:



2. To configure your calendar:
 - Click on the *Options* button. The *Options* screen displays.
 - Click on any of the headings (such as *Language* and *Date and Time Options*).
 - Follow the instructions on the screen that displays.
 - Click on the *Save Options* button to save your changes and return to the *Options* screen.
3. To change the calendar display, click on one of the date buttons (your options are *Today*, *Day*, *Work Week*, *Week*, and *Month*).
4. To schedule an event, click on the *New Event* button. Enter all appropriate information on the screen that displays and click on the *Save Event* button.
5. To import a calendar from another source:

- Click on the *Import/Export* button. The *Import/Export* screen displays:

- In the *Import Calendar* section of the screen, select the format to export from (your options are *CSV* and *Outlook*).
 - Select the file to import. Either enter the file name directly into the empty field or select it by clicking in the *Browse...* button.
 - Click on the *Import* button.
6. To export a calendar to another source:
- Click on the *Import/Export* button. The *Import/Export* screen displays.
 - In the *Export Calendar* section of the screen, select the format to export to.
 - Select the exporting time span.
 - Click on the *Export* button.

Tasks

- From the *Main WebMail Menu*, click on the *Tasks* button. Any tasks that you have will display:

2. To add a new task, click on the *New Task* button. The following screen displays:



The screenshot shows a web form titled "Adding A New Task". It contains several input fields and buttons. The "Name" field is a text box. The "Category" field is a dropdown menu with "Unfiled" selected. The "Due By" section has a radio button for "No due date" and a date/time picker for "18" of "December" "2002" at "12" "00". The "Priority" field is a dropdown menu with "1" selected. The "Completed?" field is a dropdown menu with "No" selected. The "Description" field is a large text area. At the bottom, there are two buttons: "Save Task" and "Save Changes".

3. Select the appropriate field.
4. Enter the appropriate text.
5. Click on the *Save Changes* button. Your list of tasks will appear.
6. To edit your tasks, click on the *List Tasks* button. Place a check next to any tasks that you want to edit, then select an action from the pull-down menu (*Complete Tasks*, *Delete Tasks*, *Set Task Priority*).

Memos

1. From the *Main WebMail Menu*, click on the *Memos* button. Any memos that you have will display:



The screenshot shows a web form titled "Memo Details". It contains a "Category" field with "Personal" selected. Below it is a text box containing the text "don't forget to meet the others at 3 pm". At the bottom, there are two buttons: "Modify Memo | Delete Memo" and "Back to Memo List".

2. To add a new memo, click on the *New Memo* button. The following screen displays:



3. Enter the appropriate text.
4. Click on the *Save Memo* button. Your list of memos will appear.
5. To delete your memos, click on the *List Memos* button. Place a check next to any memo that you want to delete, then select *Delete Memos* from the pull-down menu.

Mail Filters

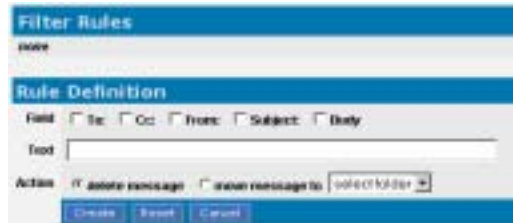
By applying rules based on message headers or content, mail filters allow you to automatically move messages to certain folders or delete messages from your inbox.

Creating a Rule

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays:



2. Click on *Edit your filter rules*. The following screen displays:

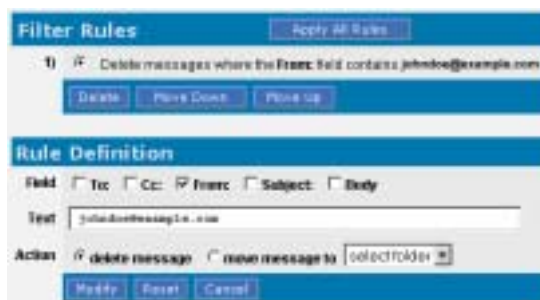


3. Select the appropriate field.
4. Enter the appropriate text.
5. Select an action. Place a check in the *delete message* box if you want mail that fits the rule to be deleted. Place a check in the *move message* box and select a folder if you want mail that fits the rule to be moved to a specific folder.
6. Click on the *Create* button.
7. The new rule displays in the *Filter Rules* section of the screen.
8. Click on the *Apply All Rules* button. Your inbox displays. As an example, if you selected *From*, entered the text *johndoe*, and selected *delete message*, all messages from johndoe will be sent directly to your trash folder.

Blacklisting a Sender

The *Blacklist* function allows you to block messages from a specific person. When you blacklist someone, you are essentially creating a rule that sends their mail to your trash folder instead of your inbox.

1. From your inbox, place a check in the message's checkbox and click on the *Blacklist* button.
2. The *Filters* screen displays, showing the new rule in the *Filter Rules* section of the screen. Click the button next to the new rule, and the *Rule Definition* window will adjust to the new rule:



3. Click on the *Apply All Rules* button. Your inbox re-displays.

Deleting a Rule

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays.
2. Select the rule you want to delete and click on the *Delete* button.

Moving Rules

Although you can apply more than one rule to a message, rules are applied in the order that they appear on the *Filter Rules* section of the screen. To move a rule up or down the list, follow these steps:

1. From the *Main WebMail Menu*, click on the *Options* button. Then click on the *Filters* button. The *Filters* screen displays.
2. Select the rule you want to move and click on the *Move Down* or *Move Up* button.

Web Server

Net Integrator's high-performance web server is based on the industry standard Apache web server and it supports CGI scripts. Perl and PHP are also integral parts of Net Integrator's web services.

For more information on Perl, go to <http://www.perl.com>.

For more information about PHP, go to <http://www.php.net>.

The Net Integrator provides web services on a *Master Web Server* and on *Virtual Web Servers*.

Master Web Server

What is the Master Web Server?

The master web server is designed to serve your Intranet site and the personal web pages of your Net Integrator users. Although it is possible to make these sites available to outside users, you may choose to keep them private for security reasons.

Master web services are provided from IP addresses assigned to Net Integrator's internal and external network interfaces. If the web server is enabled and access is granted to outside users, anyone accessing Net Integrator's internal or external IP address from a web browser can access information on the master server.

Webmaster Directory

A *Webmaster* team is created and configured as the master web server administrator. When the Webmaster team is created, a shared network directory called *Webmaster* is made available to all members of the Webmaster team, and the subdirectory *WWW* is created in the Webmaster network drive. This is the directory from which Intranet files are served. Any files saved in this directory are automatically accessible through the master web site.

The Webmaster directory also contains a *log* subdirectory (where server access and error logs are maintained) and a *cgi-bin* directory (where all CGI scripts are stored).

Configuring your Master Web Server

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP		
Enable WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No ☐ Dynamic Redirect	?
Enable secure WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No	?
Enable MySQL Server?	☒ Yes ☐ No	?
Enable users' personal home pages?	☒ Yes ☐ Only Trusted Hosts ☐ No	?
Choose a team to act as webmaster:	webmaster	?
Webmaster E-Mail address:	webmaster	
Web Proxy port: (0 to let Net Integrator choose)	0	?
Megabytes of WWW cache: (0 to disable)	0	?
Enable content filtering?	☒ Yes ☐ No [Configure]	?

[VIRTUAL DOMAINS](#)
[SSL CERTIFICATE](#)

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. Indicate whether or not you want to enable the WWW server.
 - Selecting *Yes* enables the server and allows users on the internal network and users on the Internet to access web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.

- Selecting *Only Trusted Hosts* enables the server and allows users on the internal network to access web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *No* disables the server. No one can access web pages on this server.
 - Selecting *Dynamic Redirect* enables the redirection of web connections. Dynamic redirection can be employed to circumvent blocked HTTP (WWW) ports. If this option is chosen, all WWW requests directed at the Net Integrator will be handled by a dynamic DNS server, which will automatically redirect them to a different port on the Net Integrator. This will be almost transparent for clients, who will only notice that the hostname and port have changed slightly. For Dynamic Redirect to work, you must enable Dynamic DNS (see *Chapter 20: Domain Name Services*).
3. Indicate whether or not you want to enable the secure WWW server.
- Selecting *Yes* enables the secure web server and allows users on the internal network and users on the Internet to access secure web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *Only Trusted Hosts* enables the secure web server and allows users on the internal network to access secure web pages on this server. If enabled, the WWW server will serve pages out of the webmaster's WWW directory. In addition, WWW server logs are written in the webmaster's directory.
 - Selecting *No* disables the secure web server. No one can access secure web pages on this server. Selecting *No* also means that you cannot access WebMail.
4. Indicate whether or not you want to enable the MySQL database server. MySQL is an advanced feature for users that are familiar with SQL (Structured Query Language). Refer to *Chapter 24: MySQL Server* for more information.
- Selecting *Yes* enables the MySQL server and allows users on the internal network to access personal databases and the databases of any teams that they belong to. WebMail uses the MySQL database server to store user preferences; as such, the server has to be turned on for WebMail to work.
 - Selecting *No* disables the MySQL server. Users will not have access to personal or team databases. This is the default setting.

Please Note: User and team databases are automatically created when user and team accounts are set up. MySQL databases can be used to store dynamic web page data for services such as on-line catalogues and stores.

5. Indicate whether or not you want to serve personal home pages from the WWW subdirectory (located in each user's personal network directory). You can choose to serve web pages to users on your network or to the entire Internet.
 - Select *Yes* to allow personal pages to be viewed from anywhere. For this to work, the master web server also has to be enabled
 - Select *Only Trusted Hosts* to allow personal pages to be viewed only from the local network, and not from the Internet. For this to work, the master web server also has to be enabled.
 - Select *No* to disable personal webpages.

Please Note: The address for personal home pages is in the following format:
http://server.domain/~username.
6. Although the default Webmaster team is created as the administrator of the master web server, any team can perform server maintenance tasks. If appropriate, select another team to maintain the server from the drop-down list.
7. Enter the email address of the *Webmaster* (the person who is in charge of this web site).
8. Enter the appropriate number in the *Megabytes of WWW cache* field. Refer to *Web Caching* (in this chapter) for more details.
9. Click on the *Save Changes* button.

Virtual Web Servers

Although virtual web servers allow you to host a number of web sites from the same server, these sites appear to outside users as though they are all hosted by different servers. In order to configure virtual web servers on the outside interface, your ISP has to assign you multiple IP addresses or you have to use name-based virtual web sites (which use names to distinguish between websites that share a single IP address).

Every virtual web site has to be associated with a maintenance team (which can maintain only one virtual web site). This means that for every virtual web site that you create, you also have to create a team that will maintain it. If this site is maintained by users on the local network, they can be made members of the maintenance team. If the site is maintained by outside users, they will have to use FTP to access to the web site directory. If they have an account on the server, they can use their own login name and password. If they do not have an account on the network, they have to use the team name and password.

Creating a New Virtual Web Server

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No ☐ Dynamic Redirect ?
Enable secure WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No ?
Enable MySQL Server?	☐ Yes ☒ No ?
Enable users' personal home pages?	☒ Yes ☐ Only Trusted Hosts ☐ No ?
Choose a team to act as webmaster:	webmaster ?
Webmaster E-Mail address:	webmaster ?
Web Proxy port: (0 to let Net Integrator choose)	0 ?
Megabytes of WWW cache: (0 to disable)	0 ?
Enable content filtering?	☒ Yes ☐ No [Configure] ?

VIRTUAL DOMAINS
SSL CERTIFICATE

SAVE CHANGES
CANCEL CHANGES

- Click on the *Virtual Domains* button. The *Virtual Domains* screen displays (showing all existing virtual domains):

Hostname	IP Address	Webmaster Team	Only Trusted Hosts	Allow users' personal home pages	Action
(No virtual WWW servers exist yet.)					

ADD SERVER HOME

- Click on the *Add Server* button. The *New Virtual Domain* screen displays:

Hostname of Virtual WWW Server:	virtueldomain.com	?
IP Address of Virtual WWW Server:	mc2	?
Choose a team to act as webmaster:	webmaster	?
Trusted hosts only?	☐ Yes ☐ No	?
Enable users' personal home pages?	☐ Yes ☐ No	?

SAVE CHANGES CANCEL CHANGES

- Enter your internet domain name (e.g. example.com) as the virtual domain's host name. This host name is used as a DNS entry for domain name resolution.
- The name of your Net Integrator automatically populates the *IP Address of Virtual WWW Server* field. If you want to use a different IP address, enter it in this field.
Please Note: Your ISP has to provide you with an extra IP address if you are configuring a virtual web server on an outside, untrusted interface.
- Select a team to perform Webmaster duties from the drop-down list.
- Choose whether or not to make the Virtual WWW site accessible only by trusted hosts (i.e. the local network). This way, you can easily host both an intranet and a public web site from the same server.
- Indicate whether or not you want to serve personal home pages from the WWW subdirectory (located in each user's personal network directory).
- Click on the *Save Changes* button.

Deleting a Virtual Web Server

1. Click on the *Virtual Domains* button on the *WWW Setup* screen. The *Virtual Domains* screen displays (showing all existing virtual domains).
2. Click on the appropriate server's *Delete Action* button.
3. Click *OK* to confirm the deletion in the window that displays.
Please Note: All web files for that server reside in the team's directory and will not be deleted unless the team maintaining the site is deleted as well.

Editing a Virtual Web Server

1. Click on the *Virtual Domains* button on the *WWW Setup* screen. The *Virtual Domains* screen displays (showing all existing virtual domains).
2. Click on the appropriate server's *Edit Action* button. The *Modify Virtual Domain* screen displays:

MODIFY VIRTUAL DOMAIN	
Hostname of Virtual WWW Server:	virtualdomain.com
IP Address of Virtual WWW Server:	192.168.1.102
Choose a team to act as webmaster:	webmaster
Trusted hosts only?	☒ Yes ☐ No
Enable users' personal home pages?	☒ Yes ☐ No
SAVE CHANGES CANCEL CHANGES	

3. Change the appropriate server settings.
4. Click on the *Save Changes* button.

Hosting Multiple Web Sites

If your Net Integrator will be used as a web hosting platform for a number of web sites owned by various customers, you should use the following strategy. For example, if your Net Integrator will be used to serve a web site for 'AcmeWidgets':

1. Create a team called AcmeWidgets.
2. Create a virtual web server and choose the AcmeWidgets team as the Webmaster team. Anyone from AcmeWidgets can access these files using FTP.

Secure Web Services

Secure Socket Layer (SSL) Encryption

Net Integrator's web server can serve secure web pages, which are transmitted over the Internet using Secure Socket Layer (SSL) encryption technology. All browsers on the market support SSL encryption. For SSL to work, the web server must have a file with a security certificate. This file is unique to every web server and, in order for encryption to properly work, the certificate has to be issued by a proper Certificate Authority. When the user loads a secure page, its certificate is compared to the certificate held by the Certificate Authority; if they match, the site is considered trusted, and encrypted communication can commence.

You can purchase SSL security certificates from a number of internet security companies like *Entrust* (<http://www.entrust.com>) and *VeriSign* (<http://www.verisign.com>).

Net Integrator's Security Certificates

The security certificates that Net Integrator generates can be checked for authenticity by all web browsers. The security certificate generated by Net Integrator is placed in the Webmaster directory and named *certificate.pem*.

A user loading the first secure web page from the server is warned that this security certificate is valid but that the company issuing it cannot be considered trusted. The user has to manually approve the continuation of the transaction. Despite this warning, information exchanged between the web browser and the web server cannot be viewed by others.

Please Note: If you purchase a security certificate from a Certificate Authority, delete the file automatically created by Net Integrator and replace it with the one you purchased. (See the *SSL Certificate* section in this chapter). You may also want to store a copy of the purchased certificate in a different directory.

SSL Certificate

Although a security certificate is automatically generated the first time you power-up Net Integrator, you can overwrite this certificate at any time with a 3rd party certificate purchased from a Certificate Authority.

Please Note: You can only use X.509-based certificates.

Replace with 3rd Party Certificate

1. Select WWW from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

WWW SETUP	
Enable WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No ☐ Dynamic Redirect
Enable secure WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No
Enable MySQL Server?	☐ Yes ☒ No
Enable users' personal home pages?	☒ Yes ☐ Only Trusted Hosts ☐ No
Choose a team to act as webmaster:	webmaster
Webmaster E-Mail address:	webmaster
Web Proxy port: (0 to let Net Integrator choose)	0
Megabytes of WWW cache: (0 is disable)	0
Enable content filtering?	☒ Yes ☐ No [Configure]

[VIRTUAL DOMAINS](#) [SSL CERTIFICATE](#)

[SAVE CHANGES](#) [CANCEL CHANGES](#)

- Click on the *SSL Certificate* button. The *SSL Certificate* screen displays:



CUSTOMIZE PKCS#10 CERTIFICATE REQUEST	
Country:	
State or Province:	
City or Region:	
Company Name:	
Division:	
Common Name:	localhost:8080/ssl
Email Address:	

[GENERATE REQUEST](#)

3. Fill in your personal information in the *Customize PKCS#10 Certificate Request* box:

CUSTOMIZE PKCS#10 CERTIFICATE REQUEST	
Country:	US
State Or Province:	Any State
City or Region:	Any Town
Company Name:	ABC Company
Division:	
Common Name:	bbc.webserver.net
Email Address:	youremail@domain.com
GENERATE REQUEST	

4. Click on the *Generate Request* button. A Security Alert window will appear. Click Yes to proceed.
5. The *Notices* box at the top of the screen will show that Net Integrator is generating a new certificate request based on the information you provided above, and



a new certificate request will be generated in the *PKCS#10 Certificate Request* box:



6. Copy and paste the new certificate request from the *PKCS#10 Certificate Request* box and give it to your Certificate Authority. They will use this to generate a new certificate.

- Once you have received the new certificate from your Certificate Authority, copy and paste it into the *X.509 Certificate* box:



- Click on the *Replace Certificate* button.

Web Caching

In order to improve bandwidth, the Net Integrator can temporarily store web files accessed by internal users in a cache. If a user requests any of these stored files, Net Integrator serves them from the cache instead of from the original web site. Internet bandwidth is used only to retrieve web pages that have not previously been viewed, resulting in much faster access to the Internet.

Configuring Web Caching

1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:

2. Enter the amount of data to be cached in the *Megabytes of WWW cache* field. We recommend that you allow 5-10 MB for every active user on the internal network.
Please Note: Once the cache is full, the oldest files are deleted to make space for new ones. Configuring the cache size to zero disables the web cache server.
3. Click on the *Save Changes* button.
4. For web caching to run transparently, ensure that your web browser is NOT configured to use a proxy server.
Please Note: Previous versions of Net Integrator required you to configure your browser to use a proxy server. Although you no longer need do this, web caching still functions if your browser is configured this way. However, if you plan to use web filtering in conjunction with web caching, all proxy server settings must be removed.

Positive Web Filtering

Positive Web Filtering is a service provided by Net Integrator that allows the system administrator to allow access to specific Internet sites while blocking access to all others.

Enabling the Web Filter

1. Select WWW from the *Server Setup* menu on the left side of any WebConfig screen. The WWW Setup screen displays:

WWW SETUP	
Enable WWW server?	☒ Yes ☐ Only Trusted Hosts ☐ No ☐ Dynamic Redirect
Enable secure WWW server?	☐ Yes ☐ Only Trusted Hosts ☐ No
Enable MySQL Server?	☐ Yes ☐ No
Enable users' personal home pages?	☐ Yes ☐ Only Trusted Hosts ☐ No
Choose a team to act as webmaster:	webmaster
Webmaster E-Mail address:	webmaster
Web Proxy port: (0 is let Net Integrator choose)	0
Megabytes of WWW cache: (0 is disable)	0
Enable content filtering?	☒ Yes ☐ No [Configure]

[VIRTUAL DOMAINS](#)
[SSL CERTIFICATE](#)
[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. In the *Enable content filtering* field, select Yes.
3. Click on the *Save Changes* button.

4. Click on *Configure*. The *Web Filtering* screen displays:

The screenshot displays the 'Web Filtering' configuration interface with the following sections:

- WORKSTATIONS EXEMPT FROM FILTERING**: A table with two columns: 'Workstation' and 'Action'. The 'Workstation' column contains a text input field, and the 'Action' column contains a checkmark icon.
- CONTENT FILTERING REQUESTS**: A summary bar showing 'Requests' and 'Users have requested access to 0 additional sites.' with a help icon.
- CONTENT FILTERING REQUEST DENIALS**: A summary bar showing 'Denials', '1 filter request has been denied.', a '[Show Denial List]' link, and a help icon.
- PERMITTED WEB SITES**: A table with two columns: 'Web Site' and 'Action'. The 'Web Site' column contains a text input field, and the 'Action' column contains a checkmark icon.

Below the sections is a 'REFRESH' button.

Please Note: Previous versions of Net Integrator required you to configure your browser to use a proxy server for web caching. Although you no longer need do this, web caching still functions if your browser is configured this way. However, if you plan to use web filtering in conjunction with web caching, all proxy server settings must be removed.

Providing Full Internet Access

To provide a specific user with access to all Internet sites:

1. Enter their host name or IP address in the *Workstations Exempt from Filtering* section of the screen.
2. Click on the *Accept Action* button. The user displays in the list of workstations with full access.

Adding Permitted Websites

In order for users to access a specific website, the administrator has to add it to the *Permitted Web Sites* list. To do so, follow these steps:

1. Enter the site's name in the empty *Web Site* field.
2. Click on the *Accept Action* button. The site displays in the *Permitted Web Sites* list.

Please Note: The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

Accepting Access Requests

If a user has requested access to a specific website, a notice displays in the *Content Filtering Requests* section of the screen. To accept this request:

1. Click on the *Choose Now* button. The following screen displays:



2. To accept a request, click on the *Accept Action* button. The *Web Filtering* screen re-displays, and the site displays in the *Permitted Web Sites* list.:

Please Note: The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

Denying Access Requests

If a user has requested access to a specific website, a notice displays in the *Content Filtering Requests* section of the screen. To deny this request:

1. Click on the *Choose Now* button. The following screen displays:



2. To deny a request, click on the *Delete Action* button. The *Web Filtering* screen re-displays, and the site no longer displays in the *Requests* section of the screen.

Please Note: Once a website has been denied access by the administrator, users will no longer be able to request access to it. The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

3. To see the list of denied websites, click on the *Show Denial List* link. The following screen displays:



4. Click on the *Edit Action* button to modify the website address or the reason for denial.
5. Click on the *Accept Action* button to move the site to the permitted site list

Entering Access Requests

1. Enter the website into your browser's address bar. Hit *Enter* on your keyboard. If the site you are attempting to access has not been added to the *Permitted Web Sites* list by the system administrator, the following screen displays:



2. Click on the *Request Access* button. The following screen displays:



Please Note: Once a website has been denied access by the administrator, users will no longer be able to request access to it. The administrator can include any subsection of the domain. If "www.red.blue.org" is requested, the admin can add "www.red.blue.org", "red.blue.org", or "blue.org". Any sites ending with that domain are permitted (for example, if the administrator added "red.blue.org", then "green.red.blue.org" would be allowed, but "violet.blue.org" would not be allowed).

FTP Server

The Net Integrator uses a File Transfer Protocol (FTP) server that allows users and teams to access network and web files. FTP services are automatically enabled for users on the internal network.

Anonymous FTP Server

The FTP server can be used in anonymous mode to allow uploads and downloads of files to a specific directory without authentication from the remote user. This anonymous mode of operation is commonly used for public file distribution on the Internet. For example, if your company wants to offer a brochure in electronic format, visitors to your web site should be advised to click on the FTP link to download the file from your FTP server.

Although the file can be downloaded from your web server, FTP is the preferred method because it offers superior performance for high volume and large file transfers.

When *Anonymous FTP* is enabled, Net Integrator automatically creates a team called *FTP*. Members of this team have access to the FTP directory. All files placed in this directory by team members are accessible to anyone on the Internet. Similarly, when *Anonymous Upload* is enabled, anyone on the Internet can upload their own files to the subdirectory in the FTP directory.

Enabling the FTP Server

1. Select *FTP* from the *Server Setup* menu on the left side of any WebConfig screen. The *FTP Server Setup* screen displays:

FTP SERVER SETUP				
Enable FTP file server?	☐ Yes	☐ Only Trusted Hosts	☐ No	?
Enable anonymous FTP?	☐ Yes	☐ No		?
Enable anonymous uploads?	☐ Yes	☐ No		?
Maximum number of anonymous connections:	10			?

2. Indicate whether or not you want to enable the FTP file server.
3. Indicate whether or not you want to enable anonymous FTP.
Please Note: If this option is enabled, anyone can download files from the FTP directory by using *anonymous* as the FTP login name and their email address as the password.
4. Indicate whether or not you want to enable anonymous uploads.
Please Note: If this option is enabled, anonymous users can upload files to the FTP directory. Be very careful with this option.
5. Enter the number of anonymous users that can be simultaneously connected to the FTP server. This option is used to prevent the over-utilization of Internet bandwidth. We recommend that you leave the default setting but increase the number of anonymous users if the server is often busy.
6. Click on the *Save Changes* button.

Enabling FTP Access

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main Setup* screen displays:

TEAM SETUP						
Admins	Team ID	Full Name	Members	PPTP/Dial-In	FTP	Action
	webmaster	Web Server Admin		*	*	(+) (X)

USER SETUP						
Admins	User ID	Full Name	Teams	PPTP/Dial-In	FTP	Action
*	root	System Administrator		*	*	(+) (X)

[ADD NEW USER](#)
[ADD NEW TEAM](#)

2. Click on the appropriate user or team's *Edit Action* button.
3. The *Modify Users* or *Modify Teams* screen displays.
4. Indicate whether or not you want this user or team to have FTP access in the *Allow FTP access* field.
5. Click on the *Save Changes* button.
6. Repeat steps 2-5 for any additional users or teams.

User vs. Team FTP Access

Users may log into the Net Integrator's FTP server by entering their assigned username and password in order to access their own user directory.

If the user wishes to access the directory of any team for which they are a member, the user need to user the team name in place of their username, but continue to use their individual password rather than needing use a team password.

Intelligent Disk Backup (idb)

Net Integrator takes a different approach to backup with idb technology, which is both cheaper and easier to use than conventional tape backup systems. The capacity of the idb backup unit varies with each Net Integrator model.

Although the idb system automatically performs backup procedures (without input from a system administrator), you can turn off idb and manually initiate backup procedures. Refer to *Initiating an idb Backup* (in this chapter) for more information.

Features of idb

Instead of conventional backup tapes, idb utilizes a removable high-capacity hard disk, which provides the following advantages:

- **Value** – one hard disk costs less than the five backup tapes needed to maintain a tape backup system.
- **High Capacity** – the idb backup cartridge can (in most cases) store a month or more of backup history.
- **Speed** – idb backup matches and often supersedes the backup speeds achieved by the most expensive tape systems on the market.
- **Instant Access** – regular backup tapes (like cassette tapes) are a linear medium, meaning that you have to fast-forward or rewind in order to find information. idb technology (like a compact disc) provides almost instant access to data.
- **Backup Intelligence** – you do not need a network administrator to figure out which tapes need to be loaded and when. NetIntelligence determines when a backup needs to be made, and whether the backup should be full or incremental. This decision is based on the amount of data on the main hard disk, the amount of utilized space on the idb system, the compressibility of your data, and the rate at which new data is added and current data is changed or updated. As a result, your idb system maximizes the amount of historical data that is backed up.

- **Durability** – you can backup data on the hard drive continuously without worrying that the drive will wear out.
- **Continuous Backup** – you can backup data in any sequence, and as often as every 15 minutes.
- **Hot Swap** – the ability to add and remove idb backup cartridges while the server is running. This means that you can swap idb disks without turning the server off. (*Hot Swap* is only available on Mark I and Mark II models).

Configuring idb

Your Net Integrator idb model automatically backs up your data throughout the entire day, takes care of all backup tasks for you, and notifies you via email about its progress. Although most of the idb process is automated, you can adjust several parameters that determine how and when your backups are completed.

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The following screen displays:

Please Note: This screen also has a *Restore* section not shown in the following image.

BACKUP SETUP

E-Mail backup reports to:	root@
Enable backup compression (smaller, slower)?	☒ Yes ☐ No
Backup every:	15 Minutes
Day begins at:	1:00 AM

[SAVE CHANGES](#)

BACKUP FILES

These directories can be backed up:		Backup?
Team webmaster	Web Server Admin	☒ Yes ☐ No
User jared@	Jane Doe	☒ Yes ☐ No
User jared@	John Doe	☒ Yes ☐ No
User root	System Administrator	☒ Yes ☐ No

[SAVE CHANGES](#) [PERFORM BACKUP](#)

2. Indicate whether or not you want to enable backup compression. As a general rule, compressed backup runs half as fast as a non-compressed backup but stores twice as much data.
 - If you select *Yes*, your backup is slower but takes up less space on the idb disk.
 - If you select *No*, your backup is faster but uses more space on the idb disk.
3. Select how often you want the system to perform a backup from the drop-down list.
4. Select when you want the system to perform a final back-up from the drop-down list. It is recommended that you select a time when nobody is using the system (i.e. late at night or early in the morning).
5. Enter the name of the administrator to whom backup reports should be emailed.
Please Note: If you have the SMTP server enabled, you can enter any email address in this field.
6. Choose how much information to put in the backup reports with the *Email Log Level* drop-down menu. Your options are: *Error*, *Warning* and *Information*.
Please Note: Normally backup reports will only include error messages, but you can also choose to include warnings or non-critical information. All messages are available from the system logs whether they are included in the backup reports or not.
7. The *Backup Files* section of the screen displays all of the directories that can be backed up. Indicate which directories you want to back up by selecting the *Yes* button.
8. Click on the *Save Changes* button to save your selections. The idb system automatically performs the backup procedure.

Initiating an idb Backup

Although the idb system automatically performs backup procedures (without input from a system administrator) you can turn off idb and manually initiate a backup from the control panel (found on the front of the Net Integrator) or from the *Backup* menu (located under the *Server Setup* menu).

A procedure initiated from the *Backup* menu allows you configure certain settings on the *Main Backup* screen. A backup initiated from the control panel begins a procedure with the settings that were last configured. To change the settings, you have to go to the *Main Backup* screen. If you initiate a manual backup from the control panel, there is a *Delay* setting. The setting you enter remains until you change it again.

IMPORTANT: A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Backup from the Net Integrator Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The *Main Backup* screen displays:

Please Note: This screen also has a *Restore* section not shown in the following image.

BACKUP SETUP

E-Mail backup reports to:

Enable backup compression (smaller, slower)? ☒ Yes ☐ No

Backup every:

Day begins at:

[SAVE CHANGES](#)

BACKUP FILES

These directories can be backed up:		Backup?
Team webmaster	Web Server Admin	☒ Yes ☐ No
User jaredkw	Jane Doe	☒ Yes ☐ No
User jaredkw	John Doe	☒ Yes ☐ No
User root	System Administrator	☒ Yes ☐ No

[SAVE CHANGES](#) [PERFORM BACKUP](#)

2. In the *Backup Setup* section of the screen, enter the appropriate backup parameters.
Please Note: Refer to *Configuring idb* (in this chapter) for more information on these fields.
3. The *Backup Files* section of the screen displays all of the directories that can be backed up. Indicate which directories you want to back up by selecting the *Yes* button.
Please Note: Click on the *Save Changes* button to save your selections. This does **not** initiate the backup procedure.
4. Click on the *Perform Backup* button to initiate the backup procedure. When the backup is finished, your Net Integrator automatically emails a backup report to the administrator.

Initiating a Backup from the Control Panel

1. Press the *Backup* button. The display panel shows a 10-second countdown, during which you can stop the backup process by pressing the *Cancel* button. After 10 seconds, the backup procedure commences and the display panel shows a progress bar.
Please Note: You can delay backup for up to 24 hours by pressing the *Up* and *Down* arrows during the countdown.

idb Restore

There are three restore scenarios:

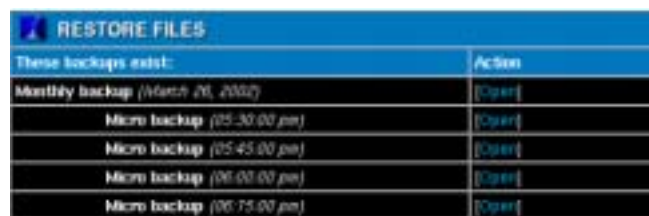
1. **Complete System Restore** – Upon total hard disk failure, perform a complete system restore to restore your system to the state of your most recent backup. After a complete system restore, all existing files are overwritten with older copies from the backup disk. However, new files saved to the hard drive *after* the backup are left untouched. A complete system restore should generally be initiated only when recovering from complete hard disk failure.
2. **Specific Directory Restore** – It is possible to restore a specific user or team network directory if these files have been lost or mistakenly deleted. A specific directory restore can only be initiated from the *Backup* menu. There are two types of specific directory restore procedures:
 - **Normal Restore** – The contents of a user or team directory get overwritten (like with a complete system restore).
 - **Safe Mode Restore** – The contents of a user or team directory get restored into a new subdirectory called *Restore* (which is created in the user or team directory). Users can browse through the content of the directory from the disk, copy any needed files, and then delete the *Restore* sub-directory.
3. **Specific File Restore** – It is possible to restore a specific user or team's network files if they have been lost or mistakenly deleted. A specific file restore can only be initiated from the *Backup* menu. There are two types of specific directory restore procedures:
 - **Normal Restore** – The file gets overwritten (like with a complete system restore)
 - **Safe Mode Restore** – The file gets restored into a new subdirectory called *Restore* (which is created in the user or team directory). Users can browse through the files from the disk, copy any needed files, and then delete the *Restore* sub-directory.
4. **Configuring Restore** - Restores system configuration.

Initiating an idb Restore

A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Directory Restore from the Net Integrator Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any Net Integrator screen. The *Main Backup* screen displays.
2. Scroll to the *Restore Files* section of the screen (which displays a list of backups and the date that the backup was performed):



RESTORE FILES	
These backups exist:	Action
Monthly backup (March 26, 2002)	[Open]
Micro backup (25:30:00 pm)	[Open]
Micro backup (25:45:00 pm)	[Open]
Micro backup (26:00:00 pm)	[Open]
Micro backup (26:15:00 pm)	[Open]

3. To view the contents of a backup file, click on the *Open* button. The following screen (showing the date and time the backup was performed, and the directories that can be restored) displays:

Please Note: The first entry in the *Restore Files* section of the screen is for *System Configuration*, which is automatically backed up every time any backup is performed. Restoring system configuration files will overwrite the current system configuration, so be **very** careful with this setting. It is recommended that you leave the default setting (*No*).



RESTORE FILES			
These directories can be restored:		Size	Restore?
jngiebel2.weavermetnuk - Tue Mar 26 17:15:00 2002			[Close]
CONFIG	System Configuration	6650	☐ Yes ☒ No
Team webmaster	Web Server Admin	4308	☐ Yes ☒ No ☐ Safe
User root	System Administrator	571	☐ Yes ☒ No ☐ Safe

PERFORM RESTORE

4. Indicate which directories you want included in the restore procedure:
 - Select *Yes* if you want this directory restored in normal mode (where the contents of the directory get overwritten)
 - Select *No* if you do not want this directory restored.
 - Select *Safe* if you want the directory restored in safe mode (where the contents of the directory are saved in the *Restore* file).

Please Note: Selecting all directories is the equivalent of performing a full system restore.

5. Click on the *Perform Restore* button to begin the restore procedure.

Initiating a File Restore from the Net Integrator Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any Net Integrator screen. The *Main Backup* screen displays.
2. Scroll to the *Restore Files* section of the screen (which displays a list of backups and the date that the backup was performed):

RESTORE FILES	
These backups exist:	Action
Monthly backup (March 26, 2002)	[Open]
Micro backup (05:30:00 pm)	[Open]
Micro backup (05:45:00 pm)	[Open]
Micro backup (06:00:00 pm)	[Open]

3. To view the contents of a backup file, click on the *Open* button. The following screen (showing the date and time the backup was performed, and the directories that can be restored) displays:

Please Note: The first entry in the *Restore Files* section of the screen is for *System Configuration*, which is automatically backed up every time any backup is performed. Restoring system configuration files will overwrite the current system configuration, so be **very** careful with this setting. It is recommended that you leave the default setting (*No*).

RESTORE FILES				
mr6.weavernet.mil - Wed Oct 29 10:22:46 2003				[Close]
These directories can be restored		Size	Restore?	Open dir?
CONFIG	System Configuration	29 k	☒ Yes ☐ No	
Team log	System Log Files	32.0 M	☒ Yes ☐ No ☐ Safe	[Open]
Team snb	snb	5471	☒ Yes ☐ No ☐ Safe	[Open]
User ftp1	ftp1	292 k	☒ Yes ☐ No ☐ Safe	[Open]
User ftp2	ftp2	1514	☒ Yes ☐ No ☐ Safe	[Open]
User ftp3	ftp3	1512	☒ Yes ☐ No ☐ Safe	[Open]
User ftp4	ftp4	1514	☒ Yes ☐ No ☐ Safe	[Open]

4. Select the appropriate directory in which the file(s) that you want to restore are located and click on the *Open* button. The following screen (showing the files that can be restored) displays:



5. Indicate which file(s) you want included in the restore procedure:
- Select *Yes* if you want this file restored in normal mode (where the file gets over-written)
 - Select *No* if you do not want this file restored.
 - Select *Safe* if you want the file restored in safe mode (where the file is saved in the *Restore* file).

Please Note: Selecting all file is the equivalent of performing a full directory restore.

6. Click on the *Perform Restore* button to begin the restore procedure.

Initiating a Restore from the Control Panel

IMPORTANT: Initiate a restore procedure from the control panel only if you want to do a complete system restore. See *idb Restore Scenarios* (in this chapter for more information).

Press the *Restore* button. The display panel shows a 10-second countdown, during which you can stop the restore process by pressing the *Cancel* button. After 10 seconds, the restore procedure commences and the display panel shows a progress bar.

idb Backup Teams

Administrators can create a “backup” team account that will grant all members of the team access to the *Backup* page in WebConfig and all associated functions. Users will have full control over backups and restores without giving them access to other administrator functions.

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays.
2. Create a team called "backup."
Please Note: See *Chapter 5: User & Team Management* for instructions on how to create a team.
3. Add any users to the "backup" team that you want to grant access to the *Backup* configuration screens in WebConfig.

idb Hot Swap

Please Note: *Hot Swap* is only available on Mark I and Mark II models. Lite and Mark IIIR models do not support *Hot Swap*.

Mark I support for *Hot Swap* requires a hardware upgrade in addition to the use of version 3.72 or higher. You cannot revert back to an older version (i.e. 3.71c) because the hardware will be different.

Mark II supports *Hot Swap* on versions 3.71 and higher. If you are currently running a server that supports *Hot Swap* you can revert back to a previous version.

There four possible Hot Swap messages that can appear on the display panel:

- **idb HotSwap:OK** - This message means that *Hot Swap* is supported and the idb disk is inactive, so it can be safely removed and replaced with another idb drive.



- **DON'T REMOVE IDB** - This message means that *Hot Swap* is supported, but the disk is currently being used for a Backup/Restore. You must wait until you see the *idb HotSwap:OK* message again before removing the disk.



- **NO BACKUP DISK!** - This message means that the Net Integrator does not detect the presence of an idb disk. You should insert an idb disk and then choose the *Update Disk Status* link on the main page of WebConfig.



Please Note: The No Backup Disk message will also display if the server is set up with all RAID disks and no idb disk(s).

- **CAN'T HOTSWAP** - This message means that *Hot Swap* is not supported on your server; therefore, you should never remove the idb disk without powering down the system.

Please Note: Lite models will always say *CAN'T HOTSWAP*.



Please Note: If you would like *Hot Swap* support, please contact your Net Integration representative.

The idb software leaves the idb disk off until it needs to perform a backup or a restore. During this time, if you remove an idb disk from the Net Integrator the display panel will continue to show *idb HotSwap:OK* until one of these events occurs:

- You manually start a backup/restore,
- You click on the *Update Disk Status* link in WebConfig, or
- The next scheduled backup begins.

After which, the Net Integrator will detect that there is no idb disk installed and change the display panel message to *No Backup Disk!*

Swapping idb Hard Disks (with Hot Swap)

1. Verify that the display panel says, "*idb HotSwap:OK.*"

Please Note: idb Hot Swapping is only available on the Mark I and Mark II models.



2. Insert the hard disk key into the lock and turn it counter-clockwise.



3. Gently take the handle and pull the idb disk out (keeping the handle horizontal).
Please Note: The tray should slide out easily. Do not use excessive force.



4. Remove the idb disk from the unit.



5. Slide the new idb disk into the drive as far as you can (keeping the handle horizontal).



6. When the idb disk has been pushed into the drive as far as it can go, gently push the handle downward. Doing so locks the disk into position.



7. Insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position.



Please Note: The Net Integrator will detect the new idb disk during either its next scheduled backup, or if you log in to WebConfig and click the Update Disk Status link.

Swapping idb Hard Disks (without Hot Swap)

1. Turn off the main power (Turn off the main power switch on the back of the Lite, Mark I and Mark II models. Unplug the main power cord on the Mark IIIR).
2. Insert the hard disk key into the lock and turn it counter-clockwise.



3. Gently take the handle and pull the disk out (keeping the handle horizontal).

Please Note: The tray should slide out easily. Do not use excessive force.



4. Remove the disk from the unit.



5. Slide the new hard disk into the drive as far as you can (keeping the handle horizontal).



6. When the disk has been pushed into the drive as far as it can go, gently push the handle downward. Doing so locks the disk into position.



7. Insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position.



8. Turn the main power back on. (The main power switch is located on the back of the Lite, Mark I and Mark II models. Plug in the main power cord on the Mark IIIR).



9. Press the power button (on the front of your Net Integrator).

Tape Backup

Some Net Integrator models are equipped with an integrated or optional external tape backup unit. Although the capacity of the tape backup unit varies with each model, you should be able to backup an entire hard disk on one backup tape.

Recommended Backup Procedure

While it is possible to backup individual user or team directories, it is highly recommended that you do a daily backup of your entire system. Make sure that you do not always perform your backup on the same tape – if the tape fails during the backup process, you are without a valid backup until you acquire a new tape. If a hard disk failure occurs during this period, you may lose all of the information that is stored on your Net Integrator. To guard against such a situation, we recommend that you follow this backup routine:

- Have a minimum of five tapes (one for each work day) on-hand for daily backups. Assign one tape for each day of the week, and label accordingly.
- At the end of each month, add a new tape to your tape collection. This new tape should replace one of the weekly backup tapes (which should then be stored off-site as a historical monthly reference). This systems allows you to have both a monthly and a weekly backup of your system.
- Follow daily backup procedures. Net Integrator's integrated tape backup unit is useless if you do not perform proper and frequent tape backups.
- Appoint someone in your office as the designated *Backup Operator*. Choose someone who will remember to initiate the backup at the end of each workday.

Initiating a Tape Backup

Users can initiate a backup procedure from the control panel (found on the front of the Net Integrator) or from the *Backup* menu (located under the *Server Setup* menu).

A procedure initiated from the *Backup* menu allows you configure certain settings on the *Main Backup* screen. A backup initiated from the control panel begins a procedure with the settings that were last configured. To change the settings, you have to go to the *Main Backup* screen. If you initiate a backup from the control panel, there is a *Delay* setting. The setting you enter remains until you change it again.

IMPORTANT: A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Backup from the Net Integrator Menu

1. Press the *Tape Eject* button. The tape containing the previous backup is ejected. Remove the tape and store it in a safe place.



2. Insert a new tape into the tape drive and push slightly. The tape is pulled into the tape drive. The door closes.



3. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The *Main Backup* screen displays:

Please Note: This screen also has a *Restore* section not shown in the following image.

The image shows two screenshots of the Net Integrator backup configuration interface. The top screenshot is the 'BACKUP SETUP' screen, which includes a header bar with a back arrow and the title 'BACKUP SETUP'. Below the header, there is a text input field labeled 'E-Mail backup reports to:' with the value 'root'. Below that is a 'Start backup in:' section with two spinners: the first is set to '0' and labeled 'hour(s)', and the second is set to '0' and labeled 'minute(s)'. At the bottom of this screen is a button labeled 'SAVE CHANGES'. The bottom screenshot is the 'BACKUP FILES' screen, also with a header bar. It contains a table titled 'These directories can be backed up:' with columns for the directory name and a 'Backup?' checkbox. The table lists four entries: 'Team webmaster' (webmaster), 'Team sales' (Sales Team), 'Team share' (General sharing directory), and 'User root' (System Administrator). Each entry has a 'Yes' radio button selected. Below the table are two buttons: 'SAVE CHANGES' and 'PERFORM BACKUP'.

These directories can be backed up:		Backup?
Team webmaster	webmaster	☒ Yes ☐ No
Team sales	Sales Team	☒ Yes ☐ No
Team share	General sharing directory	☒ Yes ☐ No
User root	System Administrator	☒ Yes ☐ No

- By default, a backup report is sent to the administrator account that was created during initial Net Integrator setup. To have the report sent to someone else, enter a different user name in the *E-Mail backup reports to* field.
- Begin a count-down to the backup procedure by entering a time frame in the *Start Backup in* field.
- The *Backup Files* section of the screen displays all of the directories that can be backed up. Indicate which directories you want to back up by selecting the *Yes* button.
Please Note: Click on the *Save Changes* button to save your selections. This does **not** initiate the backup procedure.
- Click on the *Perform Backup* button to initiate the backup procedure. When the backup is finished, the Net Integrator automatically emails a backup report to the administrator.

Initiating a Backup from the Control Panel

1. Press the *Tape Eject* button. The tape containing the previous backup is ejected. Remove the tape and store it in a safe place.



2. Insert a new tape into the tape drive and push slightly. The tape is pulled into the tape drive. The door closes.



3. Press the *Backup* button on the control panel. The display panel shows a 10-second countdown, during which you can stop the backup process by pressing the *Cancel* button. After 10 seconds, the backup procedure commences and the display panel shows a progress bar.

Please Note: You can delay backup for up to 24 hours by pressing the *Up* and *Down* directional arrows during the countdown.

If a Backup does not fit on a single tape...

A backup may not fit on a single tape if the tape is almost full or if you are backing up files that do not compress well (such as digital multimedia files). If this happens, your Net Integrator will span the backup across multiple tapes. When the first tape is filled up with data, Net Integrator closes the tape, writes a tape index, and sends an email to the backup administrator outlining which directories have been backed up and which have not.

In order to complete the backup job, the backup administrator has to put a new tape into the tape drive and press the *Backup* button (on the control panel). Your Net Integrator then continues the backup on the second tape.

Tape Restore

There are two restore scenarios:

1. **Complete System Restore** – Upon total hard disk failure, perform a complete system restore to restore your system to the state of your most recent backup tape. After a complete system restore, all existing files are overwritten with copies from the backup tape. However, new files saved to the hard drive *after* the backup are left untouched. A complete system restore should generally be initiated only when recovering from complete hard disk failure.
2. **Specific Directory Restore** – It is possible to restore a specific user or team directory if these files have been lost or mistakenly deleted. A specific directory restore can only be initiated from the *Backup* menu. There are two types of specific directory restore procedures:
 - **Normal Restore** – The contents of a user or team directory get overwritten (like with a complete system restore).
 - **Safe Mode Restore** – The contents of a user or team directory get restored into a new subdirectory called *Restore* (which is created in the user or team directory). Users can browse through the content of the directory from the tape, copy any needed files, and then delete the *Restore* sub-directory.

IMPORTANT: Restore procedures can only restore user- and team-level directories. You cannot restore selected files within a directory.

Initiating a Tape Restore

A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a Restore from the Net Integrator Menu

1. Select *Backup* from the *Server Setup* menu found on the left side of any WebConfig screen. The *Main Backup* screen displays. Scroll to the *Restore Files* section of the screen:

Please Note: If there is no backup tape in the tape drive, this section is empty. If the last backup tape is still in the tape drive, this section displays the directories backed up on that tape.

RESTORE FILES		Restore?
These directories can be restored:		
egg.spr.dns.com		
Sat Jul 11 09:31:30 2000		
CONFIG	System Configuration	☐ Yes ☐ No
User root	System Administrator	☐ Yes ☐ No ☐ Safe
User rex	Unknown file in /home	☐ Yes ☐ No ☐ Safe
User webmaster	webmaster	☐ Yes ☐ No ☐ Safe
User tom	tom	☐ Yes ☐ No ☐ Safe
User bob	Bob Smith	☐ Yes ☐ No ☐ Safe

Load Tape Index Perform Restore Now

2. Click on the *Load Tape Index* button to refresh the list of directories that can be restored. In approximately 1 to 2 minutes, an updated list (showing when the backup on this tape was performed, and the directories that are stored on this tape) displays.

IMPORTANT: The first entry in the *Restore Files* section of the screen is for *System Configuration*, which is automatically backed up every time any backup is performed. Restoring system configuration files will overwrite the current system configuration, so be **very** careful with this setting. It is recommended that you leave the default setting (*No*).

3. Indicate whether or not you want a directory included in the restore procedure. Selecting all directories for a restore is the equivalent of performing a full system restore.
 - Select *Yes* if you want this directory restored in normal mode (where the contents of the directory get overwritten)
 - Select *No* if you do not want this directory restored.

- Select *Safe* if you want the directory restored in safe mode (where the contents of the directory are saved in the *Restore* subdirectory).
4. Click on the *Perform Restore* button to begin the restore procedure.

Initiating a Restore from the Control Panel

IMPORTANT: Initiate a restore procedure from the control panel only if you want to do a complete system restore. See *Restore Scenarios* (in this chapter for more information).

1. Press the *Restore* button. The display panel shows a 10-second countdown, during which you can stop the restore process by pressing the *Cancel* button. After 10 seconds, the restore procedure commences and the display panel shows a progress bar.

Software Updates

Periodically, Net Integrator contacts our distribution servers through its Internet connection and requests an updated list of available software releases. A list of available software releases is found on the *Software Update* screen.

Upgrading your Net Integrator

It is best to upgrade your software after-hours because rebooting disconnects all users and causes all services to stop functioning until the server has restarted.

Please Note: If you are running version 3.74 or higher and you download or select another software version a *Release Notes* screen will appear. You must click on the *Continue with Download?* link at the bottom of the page in order to continue. If you are upgrading from a pre-3.74 version to 3.74 or higher, the *Release Notes* screen will not appear.

1. Select *Software Update* from the menu on the left side of any WebConfig screen. The *Software Update* screen displays, showing the software version currently running on your Net Integrator and all versions available for download:

Versions already installed:		
Version 3.72		Active
Version 3.71c		[Activate]
Versions available for download:		
Version 3.66c	[Release Notes]	[Download]
Version 3.70c	[Release Notes]	[Download]
Version 3.71c	[Release Notes]	[Download]

2. Click on the *Check Versions* button to update the list of available versions.

3. The System status screen will appear. The *SoftUpdate* line displays the progress of the download.
4. Click on a version's *Release Notes* link to access its release notes.
Please Note: The release notes outline the version's new features and provide important information that you need to know before upgrading your software. Please read the release notes carefully.
5. The new software has to be downloaded to your Net Integrator. To do so, click on the appropriate version's *Download* link. The *System Status* screen displays. The *SoftUpdate* line displays the progress of the download:



SERVICES STATUS SNAPSHOT	
Internet Status:	1 a 64.200.187.82 - Internet on eth0, via 64.201.187.84
Firewall:	iptables Firewall enabled
VPN Tunnel:	Not Enabled
SoftUpdate:	Idle

6. When the download is complete, the *SoftUpdate* line reads: *A software update has been installed. To activate it, you must Reboot the Net Integrator.*
7. Click on the *Reboot the Net Integrator* link. The following screen displays:



8. Click on the *Return* button when an IP address appears on your Net Integrator's display panel. The *System Status* screen displays. The *SoftUpdate* line asks if you want to keep the new software release:
 - Selecting *Yes* permanently installs the new operating system.
 - Selecting *No* reboots your Net Integrator and reverts to the previous operating system.

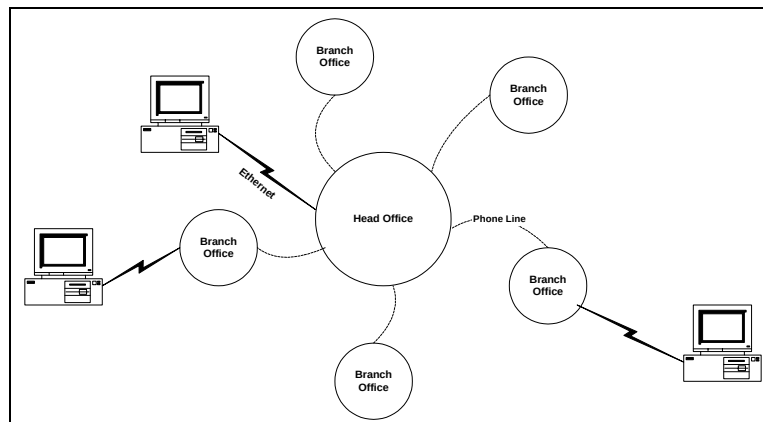
Please Note: If the newer version of the operating system is not installed properly, the server uses the old version when it reboots. If the server encounters any difficulty starting the new operating system, the previous version will start instead. If you choose not to confirm your download, and a power loss or reboot occurs, the server will revert back to the last-used operating system.

9. To revert back to the old version, select *Software Update* from the WebConfig menu. Click on the *Activate* link in the *Versions already installed* section of the screen:

Versions already installed:		
Version 3.72		Active
Version 3.71 c		[Activate]
Versions available for download:		
Version 3.66 c	[Release Notes]	[Download]
Version 3.70 c	[Release Notes]	[Download]
Version 3.71 c	[Release Notes]	[Download]

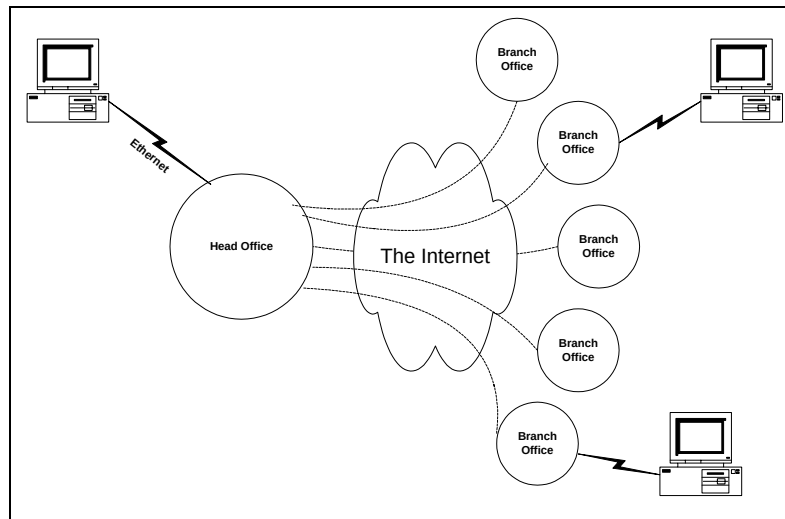
Private Networks

In the past, private networks were created by using routers to connect different office locations through dedicated phone lines. This procedure is often called a wide area network (WAN). Conventional private networks can be illustrated like this:



Virtual Private Networks

TunnelVision allows you to create a virtual private network (VPN) using the Internet instead of a WAN and dedicated phone lines for server-to-server or network-to-network connections. A VPN can be illustrated this way:



Making a Virtual Network Private

In a conventional private network, your company owns all the routers, all the computers, and all the phone lines involved. Because the only people using the network are employees, the network is secure (at least in theory).

The Internet, on the other hand, is connected to any number of businesses and organizations. As your private data passes through the Internet, it is possible that people may intercept what you are sending. In order to prevent this from happening, all of the data that passes through a VPN is encrypted with the strongest encryption technology available: 1024-bit RSA and 128-bit Blowfish algorithms. Such encryption makes it **very** difficult to intercept your transmissions.

How TunnelVision Works

A VPN allows all of the computers on two networks to communicate with each other. For this to happen, you have to first configure their subnet addresses.

When you install a Net Integrator, the IP addresses used on your local network don't really matter. Internet standards recommend that all IP addresses that are owned by internal business networks (and not used on the Internet itself) begin with 192 . 168 . The third part of the IP address specifies which private subnet number you are using, and the fourth part identifies an individual computer on the network. In special circumstances, however, you can use any subnet number at all (the first three parts of the IP address).

The important thing is that the Net Integrator and the computers on the local network have the **same** subnet number and **unique** IP addresses.

Network Address Translation (NAT)

When you communicate with other computers on the Internet, Net Integrator uses network address translation (NAT) to give each connection a valid, unique IP address that doesn't conflict with other networks.

But for a VPN, we don't want Net Integrator to use NAT, because then only two addresses will be visible: *Net Integrator #1* and *Net Integrator #2*. Instead, Net Integrator should pass addresses on each network through to the other network unchanged.

For this to happen, you need to assign different subnet numbers to each Ethernet network involved in the VPN. For example, use 192 . 168 . 1 for *Network #1* and 192 . 168 . 2 for *Network #2*. That means each computer on *Network #1* has an address starting with 192 . 168 . 1, and each computer on *Network #2* has an address starting with 192 . 168 . 2.

The Steel Pipe

To summarize, *Network #1* is connected to the Internet through Net Integrator #1 and has the subnet number 192 . 168 . 1. *Network #2* is connected to the Internet through *Net Integrator #2* and has the subnet number 192 . 168 . 2.

Gateway settings work like this: a computer on your Ethernet send packets directly to another computer if its subnet number is the same. That means that 192 . 168 . 1 . 15 will transmit directly to 192 . 168 . 1 . 46, since they are both on the same subnet. However, 192 . 168 . 1 . 15 cannot send packets directly to 192 . 168 . 2 . 20 – the subnet numbers are

similar, but they are not the same. The station then sends the data through its default gateway: *Net Integrator #1*.

Now TunnelVision can work its magic, as long as you've configured the Net Integrators to create a VPN (you'll do that later in this chapter). When Tunnel Vision starts, it creates an encrypted connection between the two Net Integrators through the Internet. This connection is sometimes called a steel pipe (because, like a true steel pipe, it's hard to see what's inside or to break through it). More often it is known as a tunnel.

Net Integrator #1 treats data addressed to *Network #2* from its local Ethernet in a special way. Rather than just passing the data to your ISP, Net Integrator encrypts it and sends it through the tunnel. When *Net Integrator #2* receives the encrypted data, it decrypts the information and forwards it on to *Network #2* as if it had arrived directly from *Network #1*. That way, *Network #1* can communicate securely with *Network #2* without any need for special changes to individual workstations.

Creating a VPN (server-to-server)

Because your Net Integrator does most of the work for you, creating a VPN is much easier than it sounds. All you have to do is create the encrypted tunnel.

Using Unique Subnet Numbers

We've already mentioned it once in this chapter, but it's so important that we'll say it again: each Ethernet network in your VPN must use a different subnet number. We recommend using any of the networks from 192.168.1 to 192.168.255, since these numbers are specifically reserved for private use.

The Master Server needs a Static IP Address

Here's the other catch. The only way to find someone on the Internet is to know their IP address (actually, if their host name is registered in the DNS system, you can use that - but DNS simply converts the host name to an IP address, so the result is the same.)

To create a connection between two Net Integrators, someone needs to act as the *Client* and someone as the *Master server*. Think of it like a phone call to your ISP: you (the client) need to know their phone number, but they (the server) don't need to know yours. With

TunnelVision, you have a similar situation: the server side (accepting a connection) needs a static IP address, while the client side can have either a static or a dynamic IP address.

Only one Net Integrator (usually the computer with the fastest Internet connection at your head office) needs to act as the server and have a static IP address. All the others can simply act as clients.

Please Note: A static IP address is guaranteed never to change, so people on the Internet can always find you. To obtain a static IP address, talk to your ISP. DDNS can be used in place of a static IP address. Refer to *Dynamic DNS* in *Chapter 20: Domain Name Services* for more information.

Configuring a TunnelVision Master Server

Ensure that the Net Integrator you are configuring as the master server has a static IP address.

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:

VPN SETUP		
Enable PPTP Server?	☐ Yes ☐ No	?
Enable Tunnel Vision?	☐ Yes ☐ No	?
Address of Master Server:		?
Tunnel Vision Password:		?
Re-enter Tunnel Vision Password:		

2. Leave the default *Enable PPTP Server* setting.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. Leave the *Address of Master Server* field empty (since the Master server does not initiate connections).
5. Enter a password that the server and client will use to prove to each other that they are trusted.
6. Re-enter the password to ensure it was entered correctly.
7. Click on the *Save Changes* button.

Configuring a TunnelVision Client

A Net Integrator doesn't need a static IP address to act as a TunnelVision client, but it needs to know the static IP address of the master server. To find this information, select *Local* from the *Network Settings* menu on the master server. On the screen that displays, click on the *Advanced...* button. Then look at the address assigned to *eth1*.

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:

VPN SETUP		
Enable PPTP Server?	☐ Yes ☐ No	?
Enable Tunnel Vision?	☐ Yes ☐ No	?
Address of Master Server:		?
Tunnel Vision Password:		?
Re-enter Tunnel Vision Password:		

[IPSEC SETUP...](#)
[SAVE CHANGES](#)
[CANCEL CHANGES](#)

2. Leave the default *Enable PPTP Server* setting.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. Enter the Master server's static IP address.
5. Enter the password that was used in step 5 of *Configuring a Master Server*.
6. Re-enter the password to ensure it was entered correctly.
7. Click on the *Save Changes* button. TunnelVision immediately begins to create the tunnel between the client and the master server. If the client and the server are connected to the Internet and everything is configured correctly, this process should only take a few seconds.

Please Note: To configure another Net Integrator as a client, simply repeat this process.

TunnelVision Status

The *System Status* screen always displays the status of active VPNs:

Please Note: You may need to click your browser's *Refresh* button to see the latest information.

SERVICES STATUS SNAPSHOT		
Internet Status:		1 a. 66.163.27.219 - Indirect on eth1, via 66.163.27.222
Firewall:		eth1: Firewall enabled.
Tunnel Vision:		mtt2 (ok)
IPsec Connections:		192.168.0.0/24 (Up), 192.168.1.0/24 (Up)
PPTP Connections:		Not enabled.

The Idle Time-out

If either end of the tunnel does not receive any data for approximately 20 minutes, it assumes that one end has disconnected from the Internet or that the tunnel is no longer needed.

If one end of the tunnel is still on-line, it will try to rebuild the connection automatically. Since this only takes a few seconds and happens only when the tunnel has been idle for a long time, this should not affect you. However, this behaviour can often cause the *VPN Tunnels* status light to turn yellow or red. This is not a sign of malfunction.

IPsec: An alternative to TunnelVision

As an alternative to TunnelVision, your Net Integrator can create an IPsec tunnel to a remote server. TunnelVision's more advanced features, such as automatic hostname and route sharing, are not provided by IPsec. We generally recommend using TunnelVision, however, for strict standards compliance, or for connecting to a server that isn't another Net Integrator, IPsec may be your only option.

Known Configurations

Net Integration's IPsec functionality is still under development (in particular to extend its usability with other products); however, it has been proven to be compatible with select products using specific configurations.

For a complete list of tested products and configurations, please go to:
http://www.net-itech.com/downloads/IPSec_Compatibility/

Adding an IPsec route

- 1 Select *IPsec Setup...* from the *VPN Setup* screen. The *IPsec Setup* screen displays:

IPSEC ROUTES					
Remote Server	Remote Subnet	Local Subnet	Enabled?	Status	Action
0.0.0.0	192.168.0.0/24	192.168.21.0/24	*	Up	⋮ X
0.0.0.0	192.168.1.0/24	192.168.21.0/24	*	Up	⋮ X

[ADD NEW ROUTE](#)
[HOME](#)

- 2 Select *Add New Route*. The *Create IPsec Route* screen displays:

CREATE IPSEC ROUTE		
Remote server:	64.80.3.12	?
Remote subnet:	192.168.21.0/24	?
Local subnet:	192.168.20.0/24	?
Remote IKE key:	sharedkey	?
Was that an RSA public key or a preshared secret key (PSK)?		☒ RSA ☐ PSK
Perfect Forward Secrecy (PFS):		☒ Yes ☐ No

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

- 3 In the *Remote Server* field, enter the IP address of the remote server you wish to connect to.
Please Note: Domain name support is not yet available.
- 4 To include a private subnet behind the remote server's firewall, enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".
Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.
- 5 Enter your *Remote IKE key* key.

- 6 From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select *PSK*.
Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
- 7 Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
- 8 Click on the *Save Changes* button.

Adding an Anonymous Incoming Connection IPsec route

- 1 Select *IPsec Setup...* from the *VPN Setup* screen. The *IPsec Setup* screen displays:

Remote Server	Remote Subnet	Enabled?	Action
No IPsec connections yet.			

ADD NEW ROUTE HOME

- 2 Select *Add New Route*. The *Create IPsec Route* screen displays:

Remote server:	0.0.0.0	?
Remote subnet:	192.168.10.0/24	?
Local subnet:	192.168.20.0/24	?
Remote IKE key:	sharedkey	?
Was that an RSA public key or a preshared secret key (PSK)?	☐ RSA ☒ PSK	?
Perfect Forward Secrecy (PFS):	☒ Yes ☐ No	?

SAVE CHANGES CANCEL CHANGES

- 3 Enter 0.0.0.0 in the *Remote Server* IP address field.

Please Note: The Net Integrator must have a static IP address.

- 4 Enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".

Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.

- 5 Enter your *Remote IKE* key key.
- 6 From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select PSK.
Please Note: Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
- 7 Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
- 8 Click on the *Save Changes* button.

Editing an IPsec route

- 1 Select the appropriate IPsec route's *Edit Action* button on the *IPsec Setup* screen.

IPSEC ROUTES					
Remote Server	Remote Subnet	Local Subnet	Enabled?	Status	Action
192.168.21.1	192.168.21.0/24	192.168.20.0/24	*	Down	

The *Modify IPsec Route* screen displays:

MODIFY IPSEC ROUTE		
Remote server:	63.80.3.12	?
Remote subnet:	192.168.21.0/24	?
Local subnet:	192.168.20.0/24	?
Remote IKE key:	sharedkey	?
Was that an RSA public key or a preshared secret key (PSK)?		?
☐ RSA ☒ PSK		
Perfect Forward Secrecy (PFS):		?
☒ Yes ☐ No		
<input checked="" type="button"/> SAVE CHANGES CANCEL CHANGES		

2. In the *Remote server* field, enter the IP address of the remote server you wish to connect to.
Please Note: Note: Domain name support is not yet available.
3. To include a private subnet behind the remote server's firewall, enter the internal IP address of the remote unit as well as the subnet in the *Remote subnet* field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24".
Please Note: To tunnel only to the remote server, and not to a subnet behind it, leave the IPsec: *Remote Server* field blank, or enter the remote server's IP address from the first field.
4. Enter your *Remote IKE key* key.
5. From the *Was that an RSA public key or a preshared secret key (PSK)?* field, select PSK.
Please Note: The RSA key feature is still under development; therefore we recommend that you only use Preshared Secret Keys (PSK).
6. Enable the *Perfect Forward Secrecy (PFS)* feature.
Please Note: It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.
7. Click on the *Save Changes* button.

Setting up Third Party IPsec Clients

With the large number of IPsec servers available, we cannot provide configuration parameters for each device on the market.

The following is the best configuration for allowing a Net Integrator to create a virtual private network (VPN) with third party devices:

Net Integrator Setup:

- **Remote server:** Enter the external IP address of the remote unit.
Please Note: Domain name support is not yet available.
- **Remote subnet:** Enter the internal IP address of the remote unit as well as the subnet. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, you would enter "192.168.10.0/24"
- **Remote IKE key:** Enter your shared key that is being used
- **Was that an RSA public key or a preshared secret key (PSK)?:** Select *PSK*
- **Perfect Forward Secrecy (PFS):** Select *Yes*

Third Party IPsec Client Setup:

- **Encryption / Tunnel:** 3DES and MD5
- **Security Association (SA) Lifetime:** set to 3600 seconds
- **Mode:** If there are different modes available, select Main Mode.
- **Private Key Secret:** Use preshared secret keys (PSK), not RSA keys or other keys such as PKI, as these are not supported on the Net Integrator.
- **Perfect Forward Secrecy:** Perfect Forward Secrecy (PFS) must be enabled on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.

Remote Access Services

What is RAS?

Remote Access Services (RAS) is a Net Integrator subsystem that allows you to access the internal network while at home or on the road. You can take advantage of RAS with:

- a VPN (which requires the Internet and a PPTP client)
- OR
- a dial-in connection (which requires a dial-up modem and a phone line).

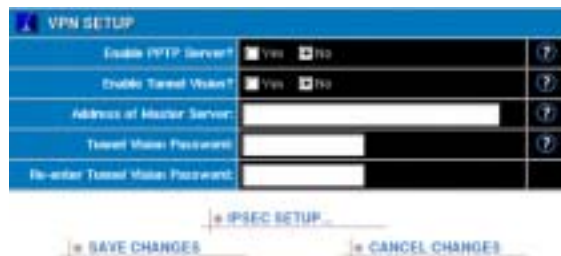
Please Note: Windows has a Point to Point Tunneling (PPTP) client built-in. You have to buy a separate software package if you are using a Macintosh.

In order to establish a remote connection, users have to have PPTP or dial-in access. Refer to *Creating Users* in *Chapter 5: User & Team Management* for more information.

PPTP - Client-to-Server VPN Service

Configuring VPN Service on Net Integrator

1. Select *VPN* from the *Network Setup* menu on the left side of any WebConfig screen. The *VPN Setup* screen displays:



2. Enable the PPTP server by selecting *Yes*.
3. Click on the *Save Changes* button.

Configuring VPN Service in Windows

Before you can establish a VPN connection, you have to install VPN service on your Windows 95/98/Me workstation. Windows 2000 and Windows XP workstations already have VPN services installed.

1. From the *Start* menu, select *Settings > Control Panel*. Double-click on the *Add/Remove programs* icon.
2. The *Add/Remove Programs Properties* screen displays. Select the *Windows Setup* tab.
3. Select *Communications* from the *Components* list and click on the *Details...* button. A second *Components* list displays, showing the communications components that are already installed and those that can be installed.
4. Scroll to *Virtual Private Networking* in the *Components* list.
 - If it already has a check, then VPN software has already been installed. Proceed to *Establishing a VPN Connection*.
 - If it doesn't have a check, you have to install the VPN software. Proceed to step 5.
5. Place a check in the *Virtual Private Networking* box and click on the *OK* button.
6. The *Windows Setup* screen re-displays. Click on the *Apply* button. The software is installed automatically. Reboot your computer when the software is finished installing.
Please Note: You may be asked to insert your Windows 95/98/Me disk for additional software components to be loaded. Simply follow the instructions provided, and refer to Microsoft Support for more information.

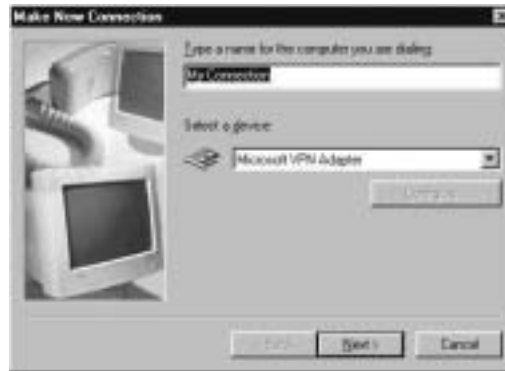
Establishing a VPN Connection

In order to establish a VPN connection to your network, you need to know your username and password and the IP address of your Net Integrator's external network interface.

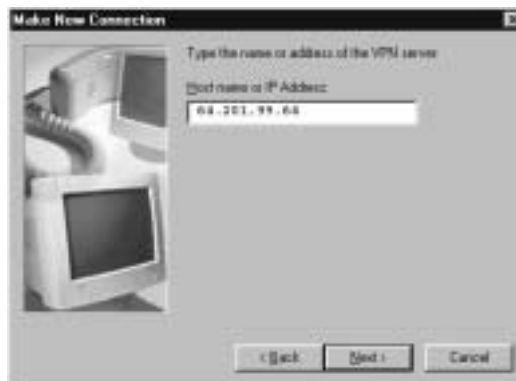
Follow these steps to establish a VPN connection in Windows 95/98/Me systems:

1. From the *Start* menu, select *Programs > Accessories > Communications > Dial-up Networking*.

2. Double-click on the *Make New Connection* icon. The following screen displays:



3. Enter a name for the VPN connection. You leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:

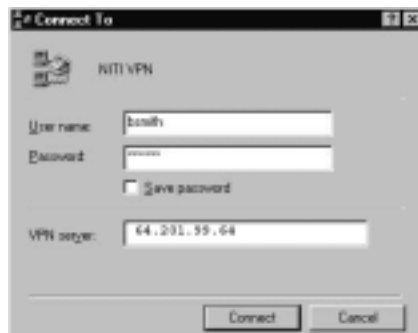


4. Enter your Net Integrator's host name or external IP address:
 - Enter a host name (such as `www.example.com`) if your Net Integrator provides DNS resolution for your domain.
 - Enter an IP address (such as `192.168.0.1`) if your Net Integrator does not provide DNS resolution. To find the external IP address, select *Local* from the *Network Setup* menu. On the screen that displays, click on the *Advanced...* button. In the *Network Devices* section of the screen that displays, look at the IP address of the un-trusted Ethernet interface (usually *Eth1*).

5. Click on the *Next* button. The following screen displays:



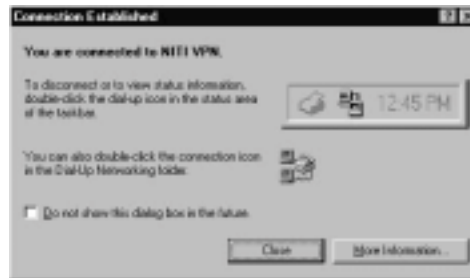
6. Click on the *Finish* button. You have created an icon that activates a VPN connection to your home network through your Net Integrator.
7. Right-click on the icon that you just created and select *Properties*. In the window that displays, click on the *Server Types* tab.
8. In the *Advanced options* section of the screen, ensure that only the following are checked:
- Enable software compression
 - Require encrypted password
 - Require data encryption.
9. In the *Allowed network protocol* section of the screen, ensure that only *TCP/IP* is checked. Click on the *OK* button.
10. Once you are connected to the Internet, establish a VPN connection to the internal network by double-clicking the icon that you created in step 6.
11. The following window displays. Enter your Net Integrator login name and password. Click on the *Connect* button:



12. The following window (showing you the progress of the connection) displays:



13. The following window displays when a VPN connection is successfully established:



14. Click on the *Close* button to minimize this window.
15. You are now connected to your local network through a secure VPN. Depending on your Internet connection, it may take longer than normal to complete network requests. The following icon (showing traffic between your workstation and the Net Integrator you are connected to) displays in the bottom right corner of your screen:



16. To terminate the VPN connection, double-click on the icon. Select *Disconnect* in the window that displays.

Disconnect a PPTP Connection

1. From the *Service Status Snapshot* screen, the *PPTP Connections:* box will display the status of all PPTP connections. If there are active connections, a *Details* link will display:

SERVICES STATUS SNAPSHOT		
Internet Status:		1 a. 24.192.219.225 - eth1, via 24.192.219.129
Firewall:		eth1: Firewall enabled.
Tunnel Vision:		Not enabled.
IPsec Connections:		Not enabled.
PPTP Connections:		1 Session. (Details)
SoftUpdate:		Idle.
Disk Status:		The primary disk (disk #1) is in standalone mode. If you remove the disk, you will lose access to your files. You can add disk #2 to your RAID array to improve redundancy. Disk #2 is being used for Intelligent Disk Backup (idb). idb disk #2 is hotswappable. (Update Status)
Web Mail:		Available at: https://hvvnetworks.com/email

2. Click on the *Details* link. The *Active PPTP Users* screen displays:

ACTIVE PPTP USERS		
Username	From IP Address	Action
hvvucong	10.42.49.102	

3. Click on the *Delete Action* button of the user whose PPTP connection you want to disconnect. A window will display asking *Are you sure you want to disconnect 'username'?* Click *OK* to disconnect the PPTP connection.

Dial-in Service

Configuring Dial-in Service on Net Integrator

1. Select *Dial-up* from the *Networking Setup* menu on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays:

Device	Type	Allow Connect?	Allow Dial In?	Action
ADSL/PPPoE/PTT on eth0	PPP-over-Ethernet or PPTP (often used on ADSL lines)			
ADSL/PPPoE/PTT on eth1	PPP-over-Ethernet or PPTP (often used on ADSL lines)			
ADSL/PPPoE/PTT on eth2	PPP-over-Ethernet or PPTP (often used on ADSL lines)			
Modem #1	Dial-up PPTP	*		

[* DETECT MODEMS](#)

2. Click on the appropriate modem's *Action* button.
3. A second *Dial-up Networking Setup* screen displays:

DIAL-UP NETWORKING SETUP	
Type of connection:	Point-to-Point Protocol (PPP) using a standard phone line
Internet Provider's Phone Number:	
Internet Account Username:	
Account Password:	
Re-order Password:	
ADVANCED OPTIONS	
Disconnect when idle for how many seconds?	300
Dial automatically when someone tries to reach the Internet?	☒ Yes ☐ Only as a last resort ☐ No
Enable Windows Dial-up Networking?	☒ Yes ☐ No
Allow Dial-in connections?	☒ Yes ☐ No

[* SAVE CHANGES](#)
[* CANCEL CHANGES](#)

4. In the *Allow Dial in connections* section, select *Yes*.
5. Click on the *Save Changes* button.

Configuring Dial-in Service in Windows

1. From the *Start* menu, select *Settings > Control Panel*. Double-click on the *Add/Remove programs* icon.
2. The *Add/Remove Programs Properties* screen displays. Select the *Windows Setup* tab.
3. Select *Communications* from the *Components* list and click on the *Details...* button. A second *Components* list displays, showing the communications components that are already installed and those that can be installed.
4. Select *Dial-Up Networking* from the *Components* list.
 - If it already has a check, then dial-in software has already been installed. Proceed to *Establishing a Dial-in Connection*.
 - If it does not have a check, you have to install the dial-in software. Proceed to step 5.
5. Place a check in the *Dial-Up Networking* box and click on the *OK* button.
6. The *Windows Setup* screen re-displays. Click on the *Apply* button. The software is installed automatically. Reboot your computer when the software is finished installing.
Please Note: You may be asked to insert your Windows 95/98/Me disk for additional software components to be loaded. Simply follow the instructions given to you.

Establishing a Dial-in Connection

When a user dials into a Net Integrator, the username will appear in the *Internet Status* field of the *System Status* screen for the duration of the connection. The administrator can terminate the connection from this screen.

In order to establish a dial-in connection to your network, you need to know your Net Integrator username and password and the phone number of a modem that is connected to an external phone line. Depending on your Internet connection, it may take longer than normal to complete network requests.

Follow these steps to establish a dial-in connection on Windows 95/98/Me systems:

1. From the *Start* menu, select *Programs > Accessories > Communications > Dial-up Networking*.
2. Double-click on the *Make New Connection* icon. The following screen displays:



3. Enter a name for the dial-in connection. You can leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:



4. Enter your area code, phone number, and country code.
5. Click on the *Next* button. The following screen displays:



6. Click on the *Finish* button. You have created an icon that activates a dial-in connection to the internal network.
7. Establish a dial-in connection by double-clicking on the icon that you created in the previous step.
8. The following window displays. Enter your Net Integrator login name and password. Click on the *Connect* button.



9. A window showing you the progress of the connection displays.
10. The following icon (showing traffic between your workstation and the Net Integrator you are connected to) displays in the bottom right corner of your screen when you are connected to the local network:



11. To terminate the connection, double-click on the icon. Select *Disconnect* in the window that displays.

Terminating a Connection from WebConfig

When a user dials into the Net Integrator, their username will appear in the *Internet Status* section of WebConfig's *System Status* screen for the duration of the connection. The administrator can choose to terminate the user's connection from this screen.

Net Integrator's firewall subsystem is entirely auto-configuring and automatically reconfigures its parameters to adapt to any Net Integrator settings. There are no user controls needed. However, you can choose to restrict outgoing traffic and view a log of all requests to traverse the firewall.

To learn more about just how sophisticated the firewall is, you can read a technical paper about it at: http://www.net-itech.com/america/products/pd_features_connectivity_firewall.htm.

Click on the *firewall-whitepaper.pdf* link at the bottom of the page. The paper will launch in Adobe Acrobat Reader.

ICSA Firewall Security Compliance

Starting with version 3.71 of Net Integrator's operating system, the Net Integrator incorporates features to be ICSA compliant. The ICSA Labs test firewall products against a standard and evolving set of criteria. Their Firewall Certification Criteria are composed of both functional and assurance requirements, and the criteria requirements define an industry-accepted standard that all products claiming to have firewalling capabilities must attain.

Traffic Denied Inbound

The firewall denies all inbound network traffic that is not for:

- Remote administration
- Private network hosts
- Service network hosts
- The firewall itself

Traffic Permitted Inbound

The firewall supports access requests for the following services, if enabled (see *Chapter 25: Log Messages* for which firewall request information is logged):

- FTP (Active and Passive Mode)
- HTTP
- HTTPS
- SMTP

Traffic Permitted Outbound

Net Integrator permits the following protocols through the firewall:

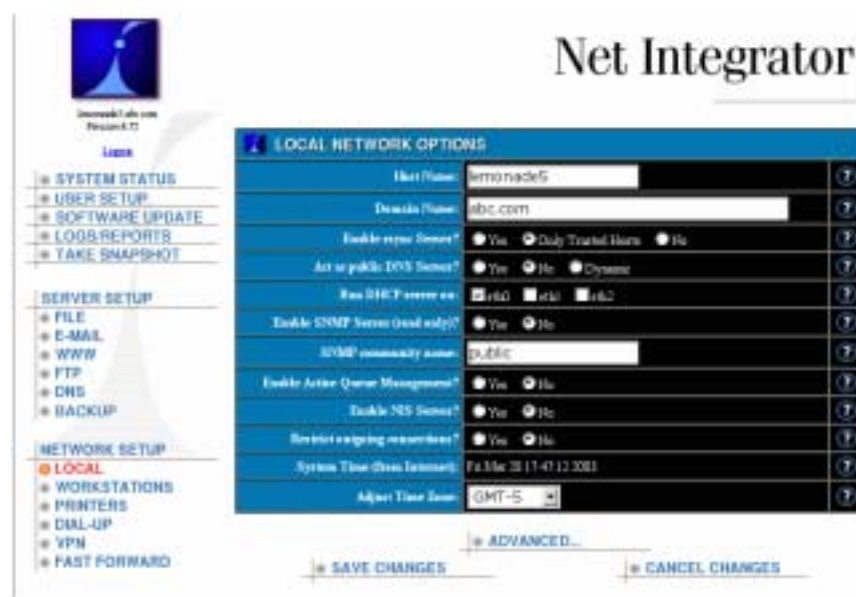
- Telnet (TCP/23) – To access resources on a Unix/Linux computer.
- FTP (TCP/20-21) – To copy files between computers.
- HTTP (TCP/80) – To make web pages available over the Internet.
- HTTPS (TCP/443) – To make secure web pages available over the Internet.
- SMTP (TCP/25) – To transfer or send email messages between servers.
- DNS (TCP and UDP/53) – To navigate the Internet using domain names instead of IP addresses.
- POP3 (TCP/110) – To read email from a single Inbox.
- IMAP (TCP/143) – To read email from a remote location.

All other non-Remote Administration traffic from both private, service and public network clients directed to or through the Net Integrator firewall will be dropped or denied.

This feature is disabled as the default setting for the Net Integrator. Once the feature is enabled, users within your network will not be able to use programs that do not adhere to the above protocols, such as ICQ.

To enable the *Restrict Outgoing Traffic* option:

1. Select *Local* under *Network Setup* from the menu on the left side of any WebConfig screen. The *Local Network Options* screen displays.



2. Enable the *Restricts Outgoing Connections* to configure your Net Integrator to only allow the above outbound ports. Disable to allow all outgoing traffic.
3. Click on the *Save Changes* button.

Please Note: Restricting outgoing traffic helps to block applications such as MSN Messenger, Yahoo Messenger, Kaza, Morpheus, etc.

Firewall Log

Please see *Chapter 25: Log Messages* for information on Firewall logs.

What is DNS?

DNS is the protocol used to convert Internet domain names into IP addresses. If DNS is configured, users can access information on the local network and the Internet using domain names instead of specific IP addresses.

Please Note: Configuring DNS services can be complicated because it often requires dealing with outside organizations called *Domain Registrars*. If you are uncertain about issues related to DNS, ask your ISP to help you.

DNS Services

Net Integrator runs two different kinds of DNS services:

- **DNS Lookup and Caching Server** – This server converts domain names (such as `www.yahoo.com`) into IP addresses and then sends the IP addresses to your browser. Net Integrator runs the DNS lookup and caching server on your local network and blocks connections to the lookup server from the Internet. There are no special options to configure the DNS lookup and caching server.
- **DNS Publishing Server** – This server adds names for your own network (such as `www.example.com`) into the global DNS system so that people can find your IP address to access your web site or to send you email. The DNS Publishing Server is quite complicated. The rest of this chapter explains how it can be configured.

-
- Net Integrator**
- Downloaded from
Version 0.12
- Learn
- SYSTEM STATUS
 - USER SETUP
 - SOFTWARE UPDATE
 - LOGS/REPORTS
 - TAKE SNAPSHOT
 - SERVER SETUP
 - FILE
 - E-MAIL
 - WWW
 - FTP
 - DNS
 - BACKUP
 - NETWORK SETUP
 - LOCAL**
 - WORKSTATIONS
 - PRINTERS
 - DIAL-UP
 - VPN
 - FAST FORWARD
- LOCAL NETWORK OPTIONS**
- | | | |
|-----------------------------------|--|---|
| Name | lemonade6 | ? |
| Domain Name | MDC019 | ? |
| Enable peer browser? | ☒ Yes ☐ Only Trained Hosts ☐ No | ? |
| Allow public DNS server? | ☒ Yes ☐ No ☐ Dynamic | ? |
| Run DHCP server via | ☒ v6 ☐ v4 ☐ v6v4 | ? |
| Enable SNMP (network card only)? | ☒ Yes ☐ No | ? |
| STMP (network card only) | SUBAC | ? |
| Enable Active Queue Management? | ☒ Yes ☐ No | ? |
| Enable PLS (network)? | ☒ Yes ☐ No | ? |
| Broadcast mapping (network card)? | ☒ Yes ☐ No | ? |
| System Time (from Internet)? | Thu Mar 28 17:47:52 201 | ? |
| Adjust Time Zone | CMT-5 | ? |
- ADVANCED
- SAVE CHANGES CANCEL CHANGES

- 214

How the DNS System Works

DNS Hierarchy

The Internet DNS server network is arranged as a hierarchy, in which a single ‘root’ domain, sometimes called dot (‘.’), links to the set of top-level domains (such as *.com* and *.org*). In turn, each of the top-level domains contains a link to each of the second-level domains (such as *net-itech.com* and *mydomain.org*). Third- and fourth-level domains are less common and are used in large organizations like universities.

You will most likely publish a second-level domain name such as *example.com*. When you do that, your DNS server (if enabled) automatically publishes the names inside *example.com*, such as *www.example.com* and *mail.example.com*.

Domain Registrars

However, there is still a part that must be done manually: in this example, you have to create a link on the *.com* server to ask your second-level domain to be referred to your Net Integrator’s IP address. To do this, you need to visit a *Domain Registrar* (such as *www.easydns.com* or *www.opensrs.org*) to make sure your domain name isn’t already being used by someone else, and give them the outside IP address of your Net Integrator.

Please Note: In order to register a domain name, your Net Integrator must have a static IP address. Most ISPs provide this service for an additional fee. DDNS can be used in place of a static IP address. Refer to *Dynamic DNS* in this chapter for more information.

After you enable your Public DNS Server and register with a Domain Registrar, people should be able to look up the IP address associated with your domain name. To test this, select *WWW* from the *Server Setup* menu, and select *Yes* in the *Enable WWW Server* field. Then ask a friend outside the local network if they can view your domain.

Dynamic DNS

Dynamic DNS is a Net Integrator feature that allows you to publish DNS entries and provide Internet services even if you have a dynamic IP address (as opposed to a static IP address).

When you register your domain with a registrar, you give them the address of the primary server and backup server owned by Net Integration Technologies (which already have static IP addresses). When your Net Integrator connects to the Internet, it automatically informs the Net Integration Technologies servers about your current IP address and asks them to publish your up-to-date DNS information.

You need to provide a Domain Registrar with the following DNS server addresses:

1. dyndns1.ivivanet.com 209.5.34.82
2. dyndns2.ivivanet.com 207.176.197.14

All you need to do then is set your *Public DNS Server* to *Dynamic*. Net Integrator does the rest.

Please Note: Dynamic DNS services require a direct connection to the Internet via a modem or router. It will not work behind a NAT device.

Manually Creating DNS Entries

Based on the servers you have enabled, your Net Integrator automatically decides which DNS names to publish. For example, if your domain name is `example.com`, and the *Enable WWW Server* option is set to *Yes* (not *Trusted Hosts Only*), then your Net Integrator automatically publishes the DNS name `www.example.com` as a pointer to your web server. Similarly, if you enable the SMTP email delivery server, it publishes the name `mail.example.com`.

Although your Net Integrator publishes names automatically, you may want to occasionally add extra names to your DNS server. You may also want to add an entry that allows people to access your site without typing `www.` before the address.

Please Note: Changing DNS information at a registrar (i.e. Network Solutions) can often take 24 - 72 hours to replicate through DNS backbone.

Types of DNS Entries

You can create four kinds of DNS entries:

- **A (address)** – Creates an entry for converting a name (such as `www.example.com`) to an IP address (such as `111.22.33.44`). This is the most common type of entry.
- **NS (copy from nameserver)** – Allows you to mirror someone else's DNS server. Every DNS server should have a backup server with an additional copy of the data. When you register a domain name, the registrar generally asks for a primary and a secondary server. If someone asks you to act as their secondary DNS server, you can add their domain name and primary server's IP address as an *NS* entry.
- **MX (mail exchanger)** – Occasionally, you may want to publish a web server and a mail server with the same name but different IP addresses. For example, you might want people to reach you by email when they send to `user@example.com`, but you might want the `example.com` web server to point to a different address. To do that, you would add Address records for `example.com` and `www.example.com` pointing to your web server, and then you would add an MX entry for `example.com` pointing to your mail server. You do not need to create a separate MX entry if it will point to the same address as the Address record.
- **DR (Dynamic Redirect)** – Dynamic redirection can be used to circumvent blocked HTTP (WWW) ports. Any WWW requests directed to the address entered as "Name" will be automatically redirected by a Dynamic DNS server to port 4201 on the site entered as "Value". This will be almost transparent for clients, who will only notice that the hostname and port have changed slightly.

Creating a DNS Entry

1. Select *DNS* from the *Server Setup* menu. The *DNS List* screen displays:

PUBLIC DNS ENTRIES				
Name	Type	Value	Origin	Action
weavernet.mall	A	192.168.10.31	Local Domain	...
ftp.weavernet.mall	A	192.168.10.31	Internal Service	...
mark2raid.weavernet.mall	A	192.168.10.31	Local Domain	...
net.weavernet.mall	A	192.168.10.31	Local Service	...
weaver.weavernet.mall	A	192.168.10.31	Local Domain	...

[ADD DNS](#)
[PRIVATE ENTRIES](#)
[HOME](#)

Please Note: To list, create or edit your private DNS entries, click the *Private Entries* button.

Private DNS entries are available only to the internal network and include hostnames of all the computers the Net Integrator can find on the local network.

Public DNS entries include the mail exchange (MX) record and entries for the un-trusted (external) network interface. Virtual WWW server DNS records will also go on the public DNS list. Most of the listings, both public and private, are automatically set up by the Net Integrator.

2. Click the *Add DNS* button. The *DNS Add* screen displays:

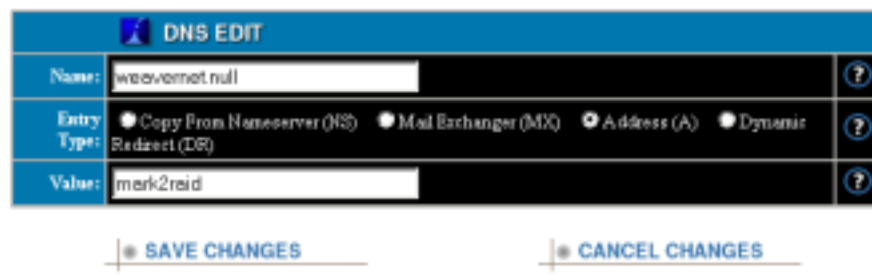
DNS ADD		
Name:		?
Entry Type:	☒ Copy From Nameserver (NS) ☐ Mail Exchanger (MX) ☒ Address (A) ☐ Dynamic ☐ Redirect (RR)	?
Value:	mark2raid	?

[SAVE CHANGES](#)
[CANCEL CHANGES](#)

3. Enter a name for the entry.
4. Select the entry type.
5. Enter the target IP address in the *Value* field.
6. Click on the *Save Changes* button.

Editing an Existing DNS Entry

1. Select *DNS* from the *Server Setup* menu. The *DNS List* screen displays.
Please Note: To edit your private DNS entries, click the *Private Entries* button.
2. Click on the entry's *Edit Action* button. The *DNS Edit* screen displays:



The screenshot shows the 'DNS EDIT' interface. It has a blue header bar with the title 'DNS EDIT' and a small icon. Below the header, there are three main sections: 'Name', 'Entry Type', and 'Value'. Each section has a text input field and a help icon (a question mark in a circle). The 'Name' field contains 'www.vornet.null'. The 'Entry Type' section has four radio buttons: 'Copy From Nameserver (NS)', 'Mail Exchanger (MX)', 'Address (A)', and 'Dynamic'. The 'Value' field contains 'mark2reid'. At the bottom of the form, there are two buttons: 'SAVE CHANGES' and 'CANCEL CHANGES', both with a small icon to their left.

DNS EDIT	
Name:	www.vornet.null ?
Entry Type:	☒ Copy From Nameserver (NS) ☐ Mail Exchanger (MX) ☐ Address (A) ☐ Dynamic ?
Value:	mark2reid ?
☒ SAVE CHANGES ☒ CANCEL CHANGES	

3. Make the appropriate changes and click on the *Save Changes* button.

What is the Workstation Viewer?

The Workstation Viewer is a Net Integrator subsystem that can list the workstations and servers that are connected through the local network or a VPN. The *Workstations* screen tells you which computers are on the network, what their names and IP addresses are, and who is logged on.

If a workstation can be administered remotely using Virtual Network Computing (described in the next section), the remote administration program can be accessed from WebConfig.

Accessing the Workstation Viewer

1. Select *Workstations* from the *Network Setup* menu on the left side of any WebConfig screen. The *Workstations* screen displays:



2. Because scanning for workstations can waste bandwidth (especially across a VPN) no workstations display in the list. Click on the *New Scan* button to view an updated list of workstations. The following screen displays:

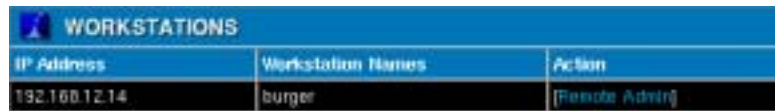


3. Click *Refresh* (on the bottom of the screen) after a few seconds to view the updated list. Workstations will only be shown in the list if they are connected to the network.

Virtual Network Computing (VNC)

Using free Windows software called Virtual Network Computing (VNC), you can configure Windows, Mac, and Unix workstations so they can be controlled remotely from a central workstation. If users need help or settings need to be changed, an administrator does not have to physically go and sit in front of the workstation in question.

Because this remote administration software is also compatible with VPNs, the administrator does not have to be on the same network or even in the same city. Computers with a VNC remote administration server installed appear with the words *Remote Admin* next to them on the *Workstations* screen:



WORKSTATIONS		
IP Address	Workstation Names	Action
192.168.12.14	burger	[Remote Admin]

Configuring VNC

There are two parts to configuring remote administration:

1. VNC Server (which should be installed on every user's workstation).
2. VNC Viewer (which should be installed on the administrator's workstation).

Once the servers and viewers are configured, clicking the *Remote Admin* link on the *Workstations* screen connects you to the remote VNC server and displays the remote desktop.

Configuring the VNC server

1. Download VNC from the Internet. Go to:
 - <http://www.uk.research.att.com/vnc/download.html>

OR

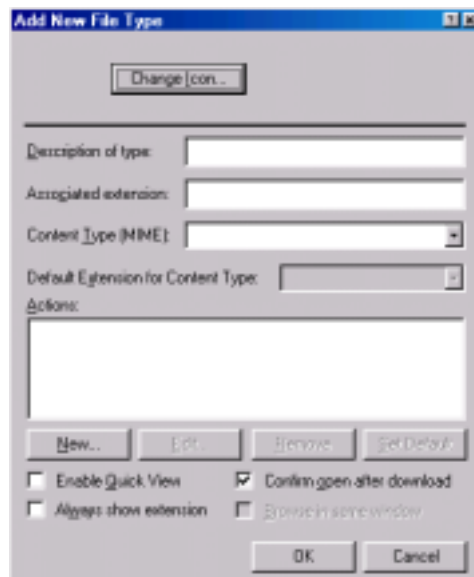
 - <http://download.cnet.com/> (and search for VNC)

Please Note: For the MAC version, go to <http://www.chromatix.uklinux.net/vnc/>

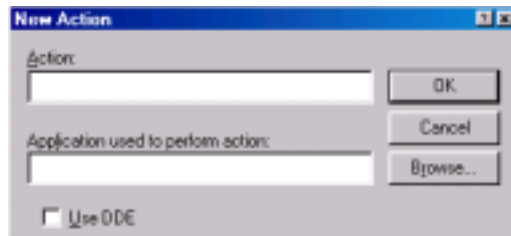
2. The file comes in a zipped format. Unzip the file in a temporary location for installation. Run the Setup program and follow the screens. Accept all defaults during the installation process.
3. When installation is finished, reboot the workstation.
4. From the Start menu, select *Applications > VNC and start VNC (App mode)*.
5. The first time you start VNC you will have to set up a password, which is needed in order to connect to your workstation.
6. When VNC is active, a small VNC icon displays in the bottom right corner of your screen.

Configuring the VNC viewer (for the Administrator's Workstation)

1. Download VNC from the Internet and configure the VNC server.
2. Look for *vncviewer.exe*, and copy it somewhere obvious (such as *c:\windows*).
3. From the Start Menu, select *Programs > Windows Explorer*.
4. From the Tools menu, select *Folder Options*. Click on the *File Types* tab. The *File Types* screen displays.
5. Click on the *New Type...* button. The *Add New File Type* screen displays:



6. Enter a description of the file type (such as *VNC Viewer Admin*) in the *Description of Type* field.
7. Enter *vnc* in the *Associated extension* field.
8. Enter *application/x-vnc* in the *Content Type (MIME)* field.
9. Click on the *New* button. The *New Action* window displays:



10. Enter *Open* in the *Action* field.
11. Enter *c:\windows\vncviewer.exe /config"%1"* in the *Application used...* field.
Please Note: *c:\windows* refers to the location where VNC has been installed. The quotations around *"%1"* are required.
12. Click on the *OK* button. VNC Viewer Admin displays in the *Registered file types* list of the *File Types* screen.

What is FastForward?

Net Integrator's FastForward technology allows you to forward Internet traffic from a specific address and interface to another address and interface. A subsystem that performs this function is usually called a *Proxy Server*.

When computers on the Internet access services on your internal, protected network, they “talk through” your Net Integrator. FastForward makes sure that these untrusted computers can only access the information and services that you want them to.

If FastForward is disabled, no-one can see anything on your local network because the Net Integrator acts as a firewall. If you enable FastForward, you are making a protected “hole” in your firewall that allows computers on the outside to access your network. To decide whether you want to use FastForward, you need to decide whether it is worth the added security risk.

Because you are affecting the firewall security of your network, it is very important that you understand what you are doing while configuring FastForward. You might want to seek qualified advice.

Introduction to TCP/IP

Entire books have been written on this subject. To save you some time, we'll try to explain everything you need in a page or two. Earlier in this guide, we talked about how each computer on the Internet must have a unique IP address. But that's not the whole story. Network protocols come in layers - IP is just one of those layers. The job of IP is to get data, split it into small chunks called packets, and then transport those packets from one computer to another on the Internet.

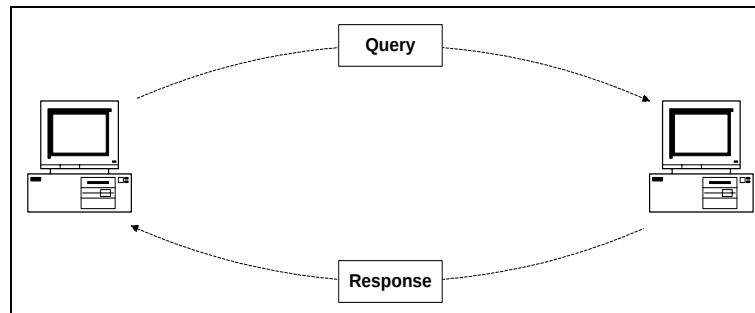
How does a computer know what to do when it receives an IP packet? Somehow, it needs to figure out what service it belongs to, and which open connection it's involved in. For that, it uses two higher-level protocols known as TCP (Transport Control Protocol) and UDP (User

Datagram Protocol). TCP and UDP introduce port numbers which specify where the data is supposed to go and how the computer is supposed to handle it.

FastForward can handle both TCP and UDP. It processes them differently from each other, but you don't need to worry about this for configuration purposes.

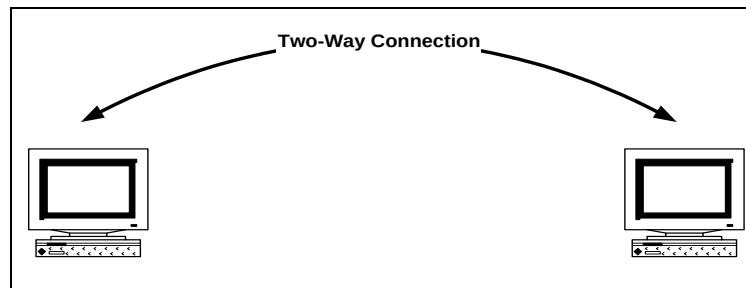
User Datagram Protocol

Using UDP is very much like sending a telegram. You receive a message, and you may send a reply. The DNS (Domain Name Service) mentioned earlier uses UDP. One computer sends a message asking to translate a name (say `www.example.com`) into a number. The answering DNS server sends a message saying that the IP address of `www.example.com` is `192.168.1.1`.



Transport Control Protocol

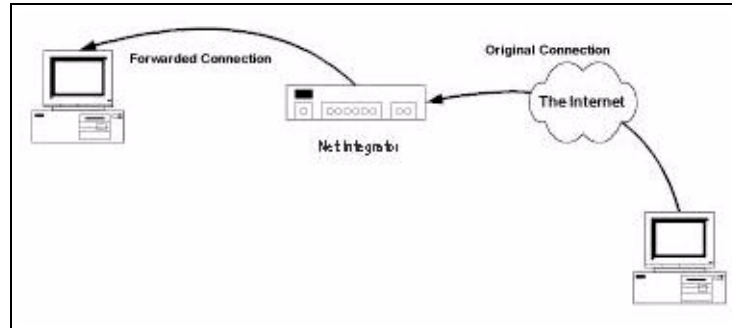
Using TCP is very much like making a telephone call. A person calls you, and you answer. You go through a introductory sequence, you have a conversation, and then you finish the call (or as we say with TCP, you close the connection). TCP is used for more complicated network tasks, like web browsing.



Proxy Servers

Net Integrator acts as a firewall, meaning that it blocks computers on the Internet from having access to your private servers.

If you want to make a service available to the outside world, FastForward controls the connection for you. When someone outside wants to access the service, they send the request to a port on your Net Integrator. FastForward then connects them to the service. This process has two connections: one from the client to the Net Integrator, and another from the Net Integrator to the server. When either the client or the server transmits information, the Net Integrator forwards it to the opposite end of the connection.



As a result, you need to know the addresses and port numbers of both the source of information and the destination of the information. Net Integrator receives connection requests from the source address and forwards them to the destination.

If you want to use FastForward, you probably already have a clear idea of what your destination address will be. The source, however, may be more difficult to determine and ultimately depends on how your IP address is configured.

Static and Dynamic IP Addresses

A person trying to access FastForward services through your Net Integrator must know your assigned IP address in order to locate you on the Internet. Each time you connect to the Internet, your ISP assigns you a IP address. Dynamic IP addresses are inconvenient for use with FastForward because your address changes each time you connect (making it difficult for your clients to find you).

If you specifically ask for one, your ISP can give you a static IP address (which never changes). Once you have a working static IP address, you can add it to a DNS server (which will convert your domain's readable name into its IP address).

Configuring FastForward

You can configure FastForward once you know your source and destination addresses. If you still aren't sure where the addresses come from, keep reading - we have a few examples a bit later on.

IMPORTANT: Remember that you decrease firewall security when you enable FastForward.

1. Login to Net Integrator with your administrator username and password. WebConfig's *System Status* page displays.
2. Select *Fast Forward* from the *Network Setup* menu. The *Fast Forward* screen displays, showing the list of addresses being forwarded

Please Note: This list may be empty if no addresses are being forwarded.



Creating a New Forward

1. Click on the *Add New Forward*. The *Add Forward* screen displays:

Add Forward		
From Address:	Net Integrator	?
From Port:		?
To Address:		?
To Port:		?

SAVE CHANGES CANCEL CHANGES

2. Enter the source address and port number in the *From Address* and *From Port* fields.
Please Note: If you enter *NetIntegrator* (with no space) as the source address, Net Integrator automatically uses your assigned address (whether it is static or dynamic). You can only attach one forward connection to any given source address and port.
3. Enter the destination address and port number in the *To Address* and *To Port* fields.
Please Note: Ensure that you have entered the destination information correctly. If you forward connections to a server that isn't answering, Fast Forward drops the connection.
4. Click on the *Save Changes* button.

Editing a Forward

1. On the *Fast Forward* screen, click on the appropriate forward's *Edit Action* button. The *Modify Forward* screen displays.
2. Change the appropriate source or destination information.
3. Click on the *Save Changes* button.

Deleting a Forward

1. On the *Fast Forward* screen, click on the appropriate forward's *Delete Action* button.
2. To confirm the deletion, click on the *OK* button on the window that displays.

Forwarding Scenarios

All this might still sound abstract and confusing. Here are a few common examples:

1. Your internal network has an email server called *Fred* running Windows NT. The address of the server is 192.168.1.5.
Set the source to Net Integrator/port 25 (which is the SMTP port) and the destination to 192.168.1.5/port 25. Now people can send email to your Net Integrator's static IP address, and it will get forwarded to your mail server.
2. If *Fred* has a DNS server on port 53, you can forward Net Integrator/port 53 to 192.168.1.5/port 53. That way, people on the Internet can look up hostnames that belong to your local network.
3. You can make WebConfig accessible from the outside world so that Net Integration Technologies Inc. technical support can get into your Net Integrator and help you with problems.
Net Integrator's port 80 is already in use for the company web server, so we'll use port 81 as the source. WebConfig* uses Port 8042 and if the destination IP is 192.168.1.1, the complete destination address is 192.168.1.1/port 8042. To access WebConfig from the outside, we would need to use a special address: `http://www.yournet-work.com:81/`

*Note - starting as of version 3.70, WebConfig actually uses port 8043 to utilize SSL encryption for added security. Thus FastFowards will need to be open to port 8043.

Here's what FastForward looks like if you choose all three of these settings:

FAST FORWARD				
From	Port	To	Port	Action
Net Integrator	25	192.168.20.5	25	...
Net Integrator	53	192.168.20.5	53	...
Net Integrator	81	192.168.1.1	8043	...

[+ ADD NEW FORWARD](#)
[+ HOME](#)

Multiple Static IP Addresses

In certain cases, you will want FastForward to treat connections differently depending on their target. For example, you might want email from `mail1.yournetwork.com` to be sent to *Fred* (your NT server) and email from `mail2.yournetwork.com` to be sent to *Barney* (your Unix server). To do this, your ISP needs to assign you multiple static IP addresses. Some ISPs may not offer this service.

If you have two static IP addresses (`207.6.60.1` and `207.6.60.2`), and you want the setup we just described, you can:

- create one forwarding entry with source `207.6.60.1` / port 25 and destination `192.168.1.5` / port 25.
- create another forwarding entry with the source `207.6.60.2` / port 25 and destination `192.168.1.6` / port 25.

Common Port Numbers

Here are a few common port numbers that you can use with FastForward.

- 22 – SSH (Secure Shell)
- 23 – Telnet
- 25 – SMTP (Simple Mail Transfer Protocol)
- 79 – Finger
- 80 – HTTP (Hypertext Transfer Protocol) - Web server
- 110 – POP (Post Office Protocol)
- 5631 – PCAnywhere
- 443 – Web server secure port (HTTPS)

Please Note: Some ports cannot be used with FastForward. For example, port 21 (FTP) does not work because it uses multiple connections that include both ports 20 and 21.

Troubleshooting FastForward

Your Net Integrator may display the following message: *An error occurred while Fast Forward tried to bind to one or more of the addresses specified.*

This message may display if:

- you are trying to forward to ports that are already being used by your Net Integrator (port 80, for example).
- FastForward has more than one entry trying to use the same source port and address. You cannot have more than one FastForward entry attached to the same source.

If you see this message, turn off the server that is already using the port. For example, to forward port 80 (the port used for web services) to another address, you would first have to shut off the web server on your Net Integrator.

The log message viewer (explained in *Chapter 25: Log Messages*) shows which Fast Forward entries did and did not work.

Disk Configuration (*idb* and *RAID*)

RAID (Redundant Array of Inexpensive Disks) is a system of backing up information that reduces risk by saving data on two or more drives. If one drive fails, your data is still safely stored on another drive. Although you do not need to know much about RAID in order to configure it on your Net Integrator, it may be helpful to know that a RAID array consisting of exactly 2 disks is called *RAID1*. A RAID array consisting of 3 or more disks is called *RAID5*.

Intelligent Disk Backup (*idb*) is a system that automatically performs backup procedures as often as every fifteen minutes without input from a system administrator. See *Intelligent Disk Backup (idb)* in *Chapter 14: Backup & Restore* for more information.

You configure your disks when you create your administrator account:

Create Administrator Account

Before you can use your Net Integrator, you must create an Administrator Account for yourself. Don't forget your password!

Create Administrator	
User ID:	root
Full Name:	System Administrator
Password:	
Re-enter Password:	
Your Domain Name:	vespernet.mll
Reserve last disk for idb backups?	☒ Yes ☐ No

Selecting *Yes* means that you reserve your last disk for Intelligent Disk Backup (idb) while using all other available disks for a RAID array. Selecting *No* means that you use all available disks for a RAID array. Refer to *Creating an Administrator Account* in *Chapter 2: Connecting to WebConfig* for more information.

Please Note: If your Net Integrator has one disk, then you cannot take advantage of idb or RAID. If your Net Integrator has exactly two disks, you can have idb backup **or** a two-disk RAID array (but not both). If you have three or more disks, you can have a two (or more) disk RAID array and idb backup **or** a RAID array with all available disks and no idb backup.

Reconfiguring your disks

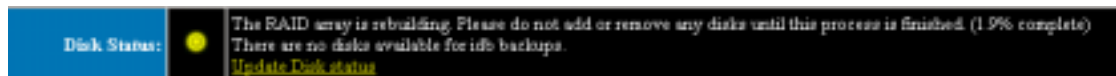
Although you configure your disks when you first setup your administrator account, it is possible to reconfigure them at a later time. The *Disk Status* section of WebConfig's *System Status* screen displays your disk status and provides you with disk reconfiguration options.

Converting an idb disk to RAID

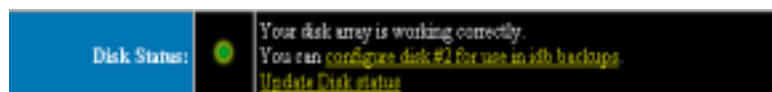
You can only convert an idb disk to part of a RAID array if your Net Integrator has exactly two disks. If you have 3 or more disks, you cannot convert an idb disk to RAID.

IMPORTANT: Converting your idb disk to part of a RAID array means that you lose idb backup capabilities. In addition, the backup information that is stored on the idb disk is permanently deleted.

1. The *Disk Status* section of the *System Status* screen has a link telling you that you can configure your last disk to your RAID array to improve redundancy. Click on this link.
2. The RAID array then begins to rebuild. This process (which can take up to two hours) does not noticeably affect the performance of your Net Integrator. Click on your browser's *Refresh* button to view an updated status of your RAID array:



- When the array has finished building, the following displays in the *Disk Status* section of the screen:



Converting a RAID disk to idb

If your RAID array is working correctly, you can convert a RAID disk to idb.

IMPORTANT: Converting your last RAID disk to idb eliminates disk redundancy (regardless of how many disks your Net Integrator has).

- The *Disk Status* section of the *System Status* screen has a link telling you that you can configure your last disk as idb. Click on this link.
- The following displays in the *Disk Status* section of the screen:



- Click on the [Reboot the Net Integrator](#) link. The following screen displays:



- When an IP address appears on your Net Integrator's display panel, click on the *Return* button. The *System Status* screen displays. The *Disk Status* section of the screen displays your new disk configuration:

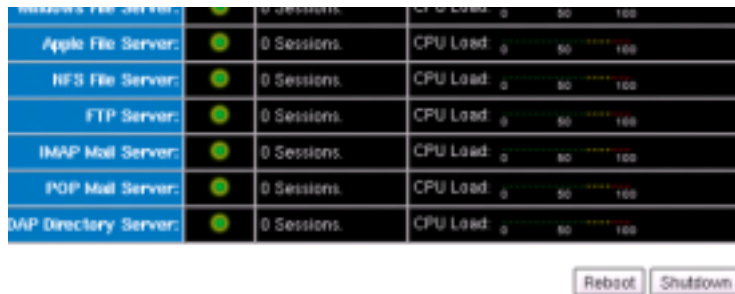


Disk Status Messages

Depending on your disk configuration, one or more of the following messages will display in the *Disk Status* section of WebConfig's *System Status* screen:

1. *The RAID array is rebuilding. Please do not add or remove any disks until this process is finished. (% complete)*

A RAID array needs to build itself the first time it is used, and rebuild when a new disk is added or when the power is turned off suddenly. This message also displays on the display panel. Always click on the *Shutdown* button (on the bottom of the *System Status* screen) before turning off your Net Integrator; failure to do so means that your RAID array will need to rebuild when you turn the box back on. Although this process does not noticeably affect the performance of your Net Integrator, it can take up to two hours to complete.



2. *Your disk array is working correctly.*
This message displays after a RAID array is finished building.
3. *No disks detected! Are your drives inserted or locked?*
This message displays when your drives are not fully inserted and properly locked or when all available drives have crashed. If your drives are not locked, insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position. If your disks have crashed, refer to *Recovering from Disk Failure* (in this chapter) for information on how to replace failed disks.
4. *The RAID array is in degraded mode. If you remove a disk, you will lose access to your files.*
This message displays if you have only one of the available drives configured in a RAID array. You can create a proper RAID array by configuring a second disk.

5. *The primary disk is in standalone mode. If you remove the disk, you will lose access to your files.*
This message displays if you have a single disk drive, if you are not using RAID, or if your two-disk RAID array is in degraded mode.
6. *There is no disk available for idb backup.*
This message displays when all available disks are configured in a RAID array.
7. *Disk #_ is being used for Intelligent Disk Backup (idb).*
This message displays when the last disk is used for idb instead of as part of a RAID array.
8. *You can add disk #_ to your RAID array to improve redundancy.*
This message displays when you have at least one un-configured disk or if your last disk is being used for idb. Click on the link to add the disk to the RAID array.
Please Note: This message appears in addition to messages 1-7.
9. *You can configure disk #_ for use in idb backups.*
This message displays if the last disk drive is un-configured. The previous message also displays, but you can only choose one of the options.
Please Note: This message appears in addition to messages 1-7.

Recovering from Disk Failure

If one of the disks in your RAID array fails:

1. Turn off the main power (Turn off the main power switch on the back of the Lite, Mark I and Mark II models. Unplug the main power cord on the Mark IIIR).
2. Remove the hard disk and replace it with a new one as soon as possible. See *Installing a New Hard Drive* (in this chapter) for more information.
Please Note: Net Integration Technologies Inc. will send you a new hard disk by overnight courier. See your Net Integrator warranty for full details.
3. Turn the main power switch back on.
4. Press the power button (on the front of your Net Integrator).

5. Connect to WebConfig:
 - a. Read the IP address on the display panel. For demonstration purposes, we will use the following address: 192.168.0.1
 - b. Enter `http://192.168.0.1:8042` into a web browser's address bar. Press *Enter* on your keyboard. WebConfig's *System Status* page displays.
6. The *Disk Status* section of the screen presents you with two options:



- To configure the new disk as part of the existing RAID array, click on *add disk #_ to your RAID array*.
 - To configure the new disk as idb, click on *configure disk #_ for use in idb backups*.
7. Depending on your choice, your Net Integrator will configure the new disk as idb or as part of your RAID array.

Disk Recovery (SystemER)

SystemER (Emergency Recovery) is an advanced set of features and procedures that:

- allows rapid data recovery in case of complete hard disk failure.
- enables Net Integrator to run in emergency mode after a hard disk failure.

Most Net Integrator units are equipped with SystemER (which is a unique Net Integrator feature that is not available from any other manufacturer).

Because hard disks are more prone to failure than solid-state devices, Net Integrator is designed in such a way that the operating system and system configuration files do not reside on the hard disk. Instead, the operating system is stored on nonvolatile solid-state memory (which provides superior reliability). A tape backup unit or idb backup along with simple backup and restore procedures allow for quick recovery in case of system failure.

If you suspect that your Net Integrator has suffered hard disk failure, contact the Net Integration technical support team immediately.

Hard Disk Failure

If technical support diagnoses your problem as hard disk failure, you will need the following in order to restore your Net Integrator:

- **Last Backup** – from which you can recover data from your last backup. If you have an idb model, you do not need a backup tape.
Please Note: All changes to system configuration, user files, and new files created by users since the last backup are not recoverable
- **New Hard Disk** – see your Net Integrator warranty for more information.
- **Hard Disk Key** – your Net Integrator has been delivered with a pair of small keys. These are used to unlock the removable hard disk tray.

Installing a New Hard Drive

1. Turn off the main power (Turn off the main power switch on the back of the Lite, Mark I and Mark II models. Unplug the main power cord on the Mark IIIR).
2. Insert the hard disk key into the lock and turn it counter-clockwise.



3. Gently take the handle and pull the disk out (keeping the handle horizontal).
Please Note: The tray should slide out easily. Do not use excessive force.



4. Remove the disk from the unit.



5. Slide the new hard disk into the drive as far as you can (keeping the handle horizontal).



6. When the disk has been pushed into the drive as far as it can go, gently push the handle downward. Doing so locks the disk into position.



7. Insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position.



8. Turn the main power back on. (Main power switch located on the back of the Lite, Mark I and Mark II models. Plug in the main power cord on the Mark IIIR).



9. Press the power button (on the front of your Net Integrator).
10. When an IP address appears on the display panel, insert the last backup tape into the tape backup drive.
Please Note: Skip this step if your last backup tape is already in the tape backup unit or if you have an idb model.
11. Press the *Restore* button on the control panel. After a 10 second countdown, the restore procedure begins and a bar graph (showing the progress of the restore procedure) appears on the display panel.
12. The length of the restore process depends on the size of your hard disk and the amount of data that has to be restored. The entire process can take up to several hours.

What is the MySQL Server?

MySQL is an advanced database administration tool that can be used to store dynamic web page data (for services such as on-line catalogues and stores), create accounting databases, and create address books. *MySQL* is an advanced feature for users that are familiar with databases and SQL (Structured Query Language). For more information, go to <http://www.mysql.com>.

If the *MySQL* server is enabled, users on the internal network can access personal databases and the databases of any teams that they belong to. Because WebMail uses the *MySQL* server to store user preference information, the *MySQL* server has to be enabled for WebMail to work properly.

Please Note: User and team databases are automatically created when user and team accounts are set up.

What is *phpMyAdmin*?

phpMyAdmin is a program that is used to administer *MySQL* databases. *phpMyAdmin* provides a user interface for *MySQL*, meaning that users can take advantage of *MySQL* databases even if they are not familiar with SQL.

Users can set-up a database in *phpMyAdmin* and use:

- Microsoft Access to access and manage the database. This is most often done for simple databases such as address books.
- OR
- PHP or Perl scripts to access and manage the database. This is most often done for dynamic web pages (which will be discussed later on in this chapter.)

Managing Databases in phpMyAdmin

Creating Database Tables

As an example, we are going to show you how to create a simple address book in *phpMyAdmin*. Later, we will show you how to manage the database in *Microsoft Access*.

1. Open an Internet browser on your workstation. Newer versions of Netscape or Microsoft browsers are recommended.
2. Read the IP address on your Net Integrator's display panel. For demonstration purposes, we will use the following address: 192.168.0.1
3. Enter `https://192.168.0.1/mysql` into the browser's address bar. Press *Enter* on your keyboard. Enter your user name and password on the screen that displays.
4. The following screen displays:



5. Select your user name from the menu on the left-hand side of the screen. The following screen displays:

Home
john (-)

Database john running on localhost

No tables found in database.

- Run SQL query/queries on database john [\[Documentation\]](#) :

☐ Show this query here again
 Or Location of the textfile :
- Create new table on database john :
 Name :
 Fields :

6. To create a new database table, enter the name of the table and the number of fields in the *Create new table...* section of the screen.

Please Note: The table name cannot contain any spaces.

7. The following screen displays:

Home
john (3)
Address Book

Database john - table Address Book running on localhost

Field	Type	Length/Values*	Attributes	Null	Default	Extra	Primary	Index	Unique	Fulltext
	TINYINT			not null			☐	☐	☐	☐
	TINYINT			not null			☐	☐	☐	☐
	TINYINT			not null			☐	☐	☐	☐

Table comments :

Table type :

* If field type is "enum" or "set", please enter the values using this format: 'A','B','C'...
 If you ever need to put a backslash ("\") or a single quote (") amongst those values, precede it with a backslash (for example 'You\'s' or 'I\'s').

8. Enter basic field information.

Field	Type	Length/Values*
Name	VARCHAR	20
Email	VARCHAR	20
Phone	VARCHAR	13

Please Note: *VARCHAR* (in the *Type* column) simply means that the entry contains numerous characters. In the *Length/Values* column, specify the maximum number of characters allowed in the entry.

9. If appropriate, select one field as *Primary* by clicking on the check-box. This prevents duplication in the address book (i.e. prevents two entries from having the same name, email address, or phone number).

Please Note: All other options (such as *Attributes*, *Null*, and *Default*) are advanced features that you are not required to fill in.

10. Click on the *Save* button. The following screen displays:

Home
john (1)
Address Book

Database john - table Address Book running on localhost

table Address Book has been created.

SQL-query: [Edit]
CREATE TABLE 'Address Book' (
 'Name' VARCHAR(20) NOT NULL,
 'Email' VARCHAR(20) NOT NULL,
 'Phone' VARCHAR(13) NOT NULL,
 PRIMARY KEY ('Name')
);

[Browse] [Select] [Insert] [Empty] [Drop]

Field	Type	Attributes	Null	Default	Extra	Action
☐ Name	varchar(20)		No			Change Drop Primary Index Unique Fulltext
☐ Email	varchar(20)		No			Change Drop Primary Index Unique Fulltext
☐ Phone	varchar(13)		No			Change Drop Primary Index Unique Fulltext

↑ W/A selected Change Or Drop

Indexes: [Documentation]

Keyname	Type	Cardinality	Action	Field
PRIMARY	PRIMARY	0	Drop Edit	Name

Create an index on 1 columns Go

Space usage:

Type	Usage
Data	0 Bytes
Index	1,024 Bytes
Total	1,024 Bytes

Row Statistics:

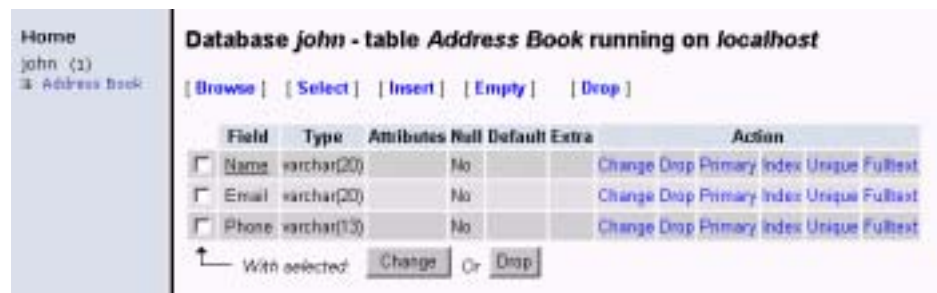
Statements	Value
Format	dynamic
Rows	0

11. On this screen, you can insert values, edit entries, and delete entries.

- To insert values for an entry, click on the *Insert* button (at the top of the screen). Enter the appropriate information into the *Value* field.
- To edit an entry, click on the *Change* button (in the *Action* section of the screen).
- To delete an entry, click on the *Drop* button (in the *Action* section of the screen).

Editing Database Tables

1. To edit a database table, log-in to *phpMyAdmin* and select the appropriate table from the menu on the left-hand side of the screen. The following screen displays:

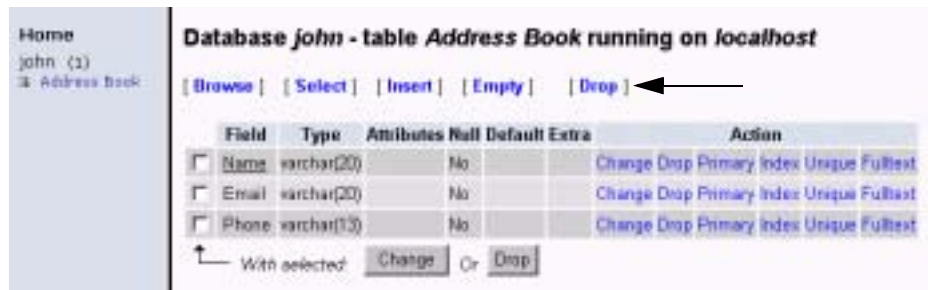


Please Note: This screen has other options not shown in this image.

2. Click on the *Change* button (in the *Action* section of the screen).
3. On the screen that displays, you can edit the following: *Field*, *Type*, *Length/Values*, *Attributes*, *Null*, *Default*, and *Extra*. Change the entry as appropriate.
4. Click on the *Save* button.

Deleting Database Tables

1. To delete a database table, log-in to phpMyAdmin and select the appropriate table from the menu on the left-hand side of the screen. The following screen displays:



Please Note: This screen has other options not shown in this image.

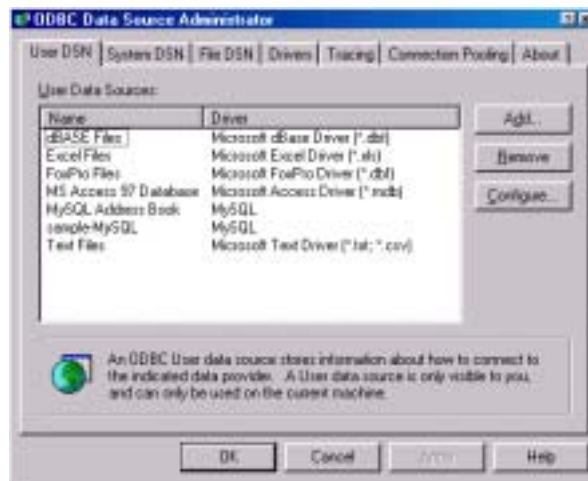
2. Click on the *Drop* button (at the top of the screen).
3. In the window that displays, click on the *OK* button.

Setting up Windows for MySQL Access

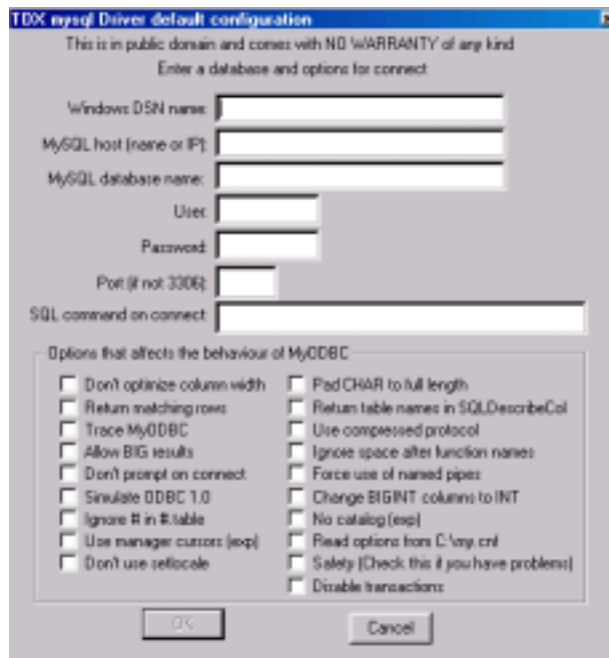
Instead of using phpMyAdmin, you can use *Microsoft Access* to access and manage database tables. We are still using the example of an address book.

1. You first have to download *MySQL ODBC* (Open Database Connectivity). Go to <http://www.mysql.com/downloads/api-mysodbc.html>.
2. On the screen that displays, click on the link for the most recent stable release.
Please Note: Always download the most recent stable release. For this example, we downloaded *MyODBC 2.50*.
3. From the *Windows Downloads* section of the screen that displays, click on the *Download* link for Windows 95/98/Me systems.
4. On the screen that displays, select the nearest server to download from.
5. In the window that displays, select *Save* (to save MyODBC to your desktop).
6. Double-click the icon on your desktop. Extract the zip file to a directory called *myodbc*.
7. Double-click on the *myodbc* folder that you created in the previous step. Double-click on *Setup.exe*.

8. The *Microsoft ODBC Setup* screen displays. Click on the *Continue* button.
9. Select *MySQL* from the *Available ODBC Drivers* list. Click on the *OK* button.
10. From the Windows Start menu, select *Settings > Control Panel > ODBC Data Source*. The *ODBC Data Source Administrator* screen displays:



11. Click on the *Add...* button. The *Create New Data Source* screen displays.
12. Select *MySQL* from the list. Click on the *Finish* button. The following screen displays:



13. On this screen, enter:

- a Windows DSN Name (such as *MySQL Address Book*)
- your Net Integrator's host name or IP address
- your MySQL database name, user name, and password.

Please Note: You do not have to worry about the other fields on this screen.

14. Click *OK* on this screen and then on the *ODBC Data Source Administrator* screen.

15. Open *Microsoft Access*.

16. Create a database named *address book*. The following screen displays:



17. Anywhere in this window, right-click your mouse. Select *Link Tables*.
18. In the *Files of Type* section of the screen that displays, select *ODBC Databases*. The *Select Data Source* screen displays.
19. Select the *Machine Data Source* tab and select *MySQL Address Book*. The *Link Tables* screen displays.
20. Select the appropriate table and click on the *OK* button. The following screen displays:



21. Make sure the appropriate table is highlighted and click on the *OK* button. The table opens in Microsoft Access.

What is a Dynamic Web Site?

Dynamic web sites, such as online stores or catalogues, use databases to store information and PHP or Perl script to produce the web page based on the data stored in the database. This allows the changing information to be reflected on the site as it changes.

Please Note: Dynamic web sites require advanced knowledge of PHP or Perl script, and it is advisable that you seek the help of a qualified programmer to create your own.

Generating Dynamic Web Sites

The following PHP script is used to render the example address book into a dynamic web site.

1. Enter the following script into a text file and save it as *addressbook.php*:

```
<table>
<?php
mysql_connect("localhost", "john", "password");
mysql_select_db("john");
$result = mysql_query("SELECT * FROM AddressBook");
while ($line = mysql_fetch_array($result))
list ($name[],$phone[]) = $line;
for ($i = 0; $i < sizeof($name); $i++)
echo "<tr><td>$name[$i]</td><td>$phone[$i]</td></tr>\n";
?>
</table>
```

2. In the Windows Network Neighborhood, copy the script in John's WWW folder (on the local server).
3. Open an Internet browser on your workstation. In the address bar of the browser, enter: `http://servername/~john/addressbook.php`.
4. The address book opens in the browser.

Accessing Log Messages

Net Integrator keeps a log that displays the messages from all of Net Integrator's subsystems. To view the log from the firewall subsystem, please refer to the *Firewall Log* section below.

To access this log:

1. Select *Logs/Reports* from the menu on the left side of any WebConfig screen. The *Log Messages* screen displays:

Time	Source	Pri.	Message
9:41:39 AM	Weaver	Notice	Weaver version 3.72 is starting
	CEM Manager	Notice	Manufacturer: Net Integrator Technologies CEM Options: IDS, Taps, etc CEM Info String: WL9206R6B200QH80000E HPHIMUPITQW8KPHWIKSHVIOE AEU8MCMWTF
	Traffic Staging	Info	Active queue management is disabled
	Hot Interface	Info	Changing tap0 address to 10.42.41.45 (12 bit)
9:41:38 AM	Weaver	Info	Successfully loaded the X.509 security certificate
	LCD Panel	Info	Initializing Front Panel
	HotSwap	Notice	HotSwap info verified: hsg on 10.40.56.4000110
		Info	LCD info HotSwap: OK
		Info	LCD info HotSwap: OK
	Fast Forward	Info	Fast Forward proxy server version 1.81
9:41:31 AM	WanUp	Info	No WanUp card found
	Weaver	Notice	LCD/C configuring: X SoftUpdate
		Notice	LCD/C configuring: X Network Map
	Net Map	Notice	Found a network interface called 'eth1'
		Notice	Found a network interface called 'eth0'
	Weaver	Notice	LCD/C configuring: X Modem
	WanDown	Info	Initializing modem device
		Info	Initializing modem device
	Weaver	Notice	LCD/C configuring: X
		Notice	LCD/C configuring: Net interfaces
	Net Map	Notice	Found a network interface called 'tap0'
		Notice	Found a network interface called 'tap0'
		Notice	Found a network interface called 'tap0'

Please Note: Information messages display on a black background. Warning messages display on a yellow background. Error messages display on a red background.

Customizing Message Display

The *Highlight* drop-down menu allows you to highlight messages coming from a specific Net Integrator subsystem (such as *Disk Manager* and *Fast Forward*), making them much easier to see. To customize your message log display:

1. Select a subsystem from the *Highlight* drop-down menu.
2. Select an option from the *Priority* drop-down list.
Please Note: The *Priority* list customizes what kind of message is highlighted. By default, only messages that show a change in the system display. However, you can make error messages and debug messages display.
3. Click on the *Apply* button. The appropriate messages are highlighted.

Firewall Log

For ICSA firewall compliance, Net Integrator logs requests to send traffic through the firewall. Please see *Chapter 19: Firewall Services* for more information on Net Integrator's firewall. The following firewall information is logged:

- All permitted inbound access requests from public network clients that use a service identified in the security policy hosted on the Net Integrator itself or on a private or service network server;
- All permitted outbound access requests from private and service network clients that use a service identified in the security policy on a public network server;
- All access requests from private, service and public network clients to traverse the Net Integrator firewall that violate the security policy;
- All access requests from private, service and public network clients to send traffic to the Net Integrator itself that violate the security policy;
- All attempts to authenticate at an Administrative Interface on the Net Integrator itself;
- All access requests from private, service and public network clients to send traffic to the Net Integrator itself on the port or ports used for Remote Administration;
- Each Startup

The logs contain the following information:

- Date and Time - when the event occurred with an accurate Date/Timestamp;
- Protocol - TCP, UDP, ICMP, other; Source IP Address;
- Destination IP Address;
- Destination Port (TCP and UDP) or Message Type (ICMP);
- Disposition of the event. (Blocked, allowed, etc.)

To view the firewall log, you must be a member of the *Log* team. The firewall log file will then appear in team folder on the Net Integrator. This team is automatically created by the Net Integrator.

To add a user to the *Log* team:

1. Select *User Setup* from the menu on the left side of any WebConfig screen. The *Main User Setup* screen displays:

TEAM SETUP						
Action	Team ID	Full Name	Members	Permissions	FTP	Action
	fw	Firewall/FW Admin	none	*	*	⊖ ⊕
	log	Log	none, logviewer	*	*	⊖ ⊕
	study	Net	none	*	*	⊖ ⊕
	webmaster	Webmaster team		*	*	⊖ ⊕

USER SETUP						
Action	User ID	Full Name	Teams	Permissions	FTP	Action
*	root	System Administrator		*	*	⊖ ⊕
	logviewer	Any	log	*	*	⊖ ⊕
	none	None Code	(All Teams)	*	*	⊖ ⊕
	oldwebmaster	Ultimate's Old Webmaster		*	*	⊖ ⊕
	no	no		*	*	⊖ ⊕
	webmaster2	webmaster2		*	*	⊖ ⊕

[+ ADD NEW USER](#)
[+ ADD NEW TEAM](#)

2. Click on the appropriate user's *Edit Action* button. The *Modify Users* screen displays:

MODIFY USER	
User ID:	NET/USER
Full Name:	Any User
Password:	XXXXXXXXXX
Re-enter Password:	XXXXXXXXXX
Administrator Access:	☐ Yes ☐ No
Allow FTP Access:	☐ Yes ☐ No
Allow VTN (FTTP) and Dial-In Access:	☐ Yes ☐ No
Allow Exchange/IM License:	☐ Yes ☐ No
Automatically mount files as:	X
Join Teams:	☐ backup ☐ exchange-admin ☐ log ☐ mailbox ☐ mailing ☐ postmaster ☐ webmaster
Test E-Mail:	[None]

3. Choose the *Log* team in the *Join Teams* field.
4. Click on the *Save Changes* button.
5. Access the team folder on the Net Integrator.

What is NFS?

NFS (Network File System) is a protocol invented by Sun Microsystems that allows clients using UNIX and similar operating systems to mount file systems from remote servers. This chapter is for advanced users that are familiar with UNIX and similar operating systems.

Please Note: Refer to <http://www.linuxdoc.org/HOWTO/NFS-HOWTO/> for more information on NFS.

Installing and Configuring *ugidd*

If your user ID on the local system is different than your user ID on the Net Integrator, you will not be able to access mounted directories. To avoid this problem:

1. Install *ugidd* (an application that provides user name and ID information to NFS) on your local system.
2. Select *File* from the *Server Setup* menu on the left side of any WebConfig screen. The *File Server Setup* screen displays. In the *Mapping scheme for NFS* field, select *ugidd*. Click on the *Save Changes* button.

Please Note: If you are using NIS (Network Information Server) or a similar application that provides usernames and IDs to the network, you generally do not need *ugidd*.

Mounting an NFS directory

In order to mount a directory, you must have super-user privileges. Follow these steps to mount an NFS directory:

1. If necessary, install *ugidd* on your workstation.
2. From a shell prompt, enter *showmount -e weaver*.
Please Note: This step is optional. If you already know what directories you are able to mount, proceed to step 3.
3. At the prompt, enter (for example) *mount (NFSdir) (localdir)*.
Please Note: *localdir* is the path to an existing directory on the local network. *NFSdir* is specified as *hostname:/path/directory*. For example, to mount the home directory of the user *josefk* under the local directory */mnt/josefk*, enter the following information:
mount weaver:/export/home/josefk /mnt/josefk

Unmounting an NFS Directory

You should unmount when you are done with a mounted directory or when you are going to logout. From a shell prompt, enter (for example) *umount /mnt/josefk*.

What is rsync?

It stands for **remote synchronization**. rsync is a utility that provides a very fast method for remote files to be kept in synchronization with the files on the Net Integrator. It does this by sending just the differences in the files to the remote site, without requiring both sets of files to be present beforehand. rsync can only be utilized with a unix type remote system.

Using rsync

The rsync server must be enabled using WebConfig. The option is located in the **LOCAL** configuration page.

From the remote unix system you need to mount your home directory as follows: “mount -t nfs server:/export/home/username /tmp/username”

This will mount the “username” home directory from the Net Integrator “server” to the destination directory of /tmp/username This has to be done as the root user on the remote unix system. To access the directory that was just mounted the userid (uid) has to match for the user that is accessing the directory or they will get a permission denied error. You can get the UID from the Net Integrator’s password (/etc/passwd) file and these should match to the uid on the local unix system. To get around the uid problem you can enable the **Mapping scheme for NFS**: to be ugidd on the Net Integrator system and then install ugidd daemon on the remote unix system. You can then access the files as long as the user id is the same.

Once the directory has been mounted, you can synchronize the directory by issuing the following command on the remote unix station: “rsync -zav username@server::username/. /tmpdir/.”

This will use the rsync protocol to sync “usernames” home directory from a Net Integrator system called ‘server’ to /tmpdir/ on the local machine using the userid ‘username’.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 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.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program 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.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public 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.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

The Net Integrator uses a number of software programs that are licensed under various open source licenses. We would like to thank all of the contributors to these projects, and to acknowledge those licenses here:

Linux Kernel	GNU Public License v2
apache	Apache Open Source License
ash	BSD License w/ Copyright: Copyright (c) 1991, 1993 The Regents of the University of California. All rights reserved.
bzip2	BSD License
busybox	GNU Public License v2
courier-imap	GNU Public License v2
dhcpcd	BSD License
FreeS/Wan	GNU Public License v2
ftp	BSD License
genromfs	GNU Public License v2
getline	BSD License
horde	GNU Public License v2
imp	GNU Public License v2
iptables	GNU Public License v2
lilo	GNU Public License v2
lvm	parts GNU Public License v2, and others GNU Lesser Public License
mkcramfs	GNU Public License v2
mysql	parts GNU Public License v2, and others GNU Lesser Public License
netatalk	GNU Public License v2
Debian nfs-server	mostly GNU Public License v2

NIS	GNU Public License v2
openldap	GNU Public License v2
perl	GNU Public License v1, Artistic Public License
php4	The PHP License, version 2.02
phpmyadmin	GNU Public License v2
portmap	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
pppd	BSD License for parts, others GNU Public License v2
pptp/pptpd	GNU Public License v2
proftpd	GNU Public License v2
raidtools	GNU Public License v2
rdate	BSD License
rp-pppoe	GNU Public License v2
rsync	GNU Public License v2
samba	GNU Public License v2
telnet/telnetd	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
socks4	BSD License with acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
wanpipe	GNU Public License v2
zlib	zlib License

If you wish the source code to any of the above programs that have been licensed under the GNU Public License, or the GNU Lesser Public License, or any other license that requires source distribution please send a blank CD, along with a pre-paid return postage voucher to:

Net Integration Technologies
7300 Warden Ave, Suite 106
Markham, Ontario, CANADA
L3R 9Z6

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 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.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete

object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the

same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and

separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the

Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents

of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library 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.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of pro-

protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public 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.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND

PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

The “Artistic License”

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution pro-

vided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly
jloup@gzip.org

Mark Adler
madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](ftp://ds.internic.net/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](ftp://ds.internic.net/rfc/rfc1952.txt) (gzip format).

Apache Public License

Copyright (c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR

ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see <http://www.apache.org/>.

The PHP License, version 2.02

Copyright (c) 1999, 2000 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior permission from the PHP Group. This does not apply to add-on libraries or tools that work in conjunction with PHP. In such a case the PHP name may be used to indicate that the product supports PHP.
4. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
5. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net/>".
6. The software incorporates the Zend Engine, a product of Zend Technologies, Ltd. ("Zend"). The Zend Engine is licensed to the PHP Association (pursuant to a grant from Zend that can be found at <http://www.php.net/license/ZendGrant/>) for distribution to you under this license agreement, only as a part of PHP. In the event that you separate the Zend Engine (or any portion thereof) from the rest of the software, or modify the Zend Engine, or

any portion thereof, your use of the separated or modified Zend Engine software shall not be governed by this license, and instead shall be governed by the license set forth at <http://www.zend.com/license/ZendLicense/>.

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see [<http://www.php.net>](http://www.php.net).

Copyright (c) 1989, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

ADSL	Asymmetric Digital Subscriber Line ADSL uses standard phone lines to deliver high-speed data communications. ADSL uses the portion of a phone line's bandwidth not utilized by voice, allowing for simultaneous voice and data transmission.
Bandwidth	This term describes information-carrying capacity of telephone or network wiring. Bandwidth is usually measured in bits per second.
Bit	Binary Digit The smallest unit of computerized data. A bit is represented as either 1 or 0.
Cable Modem	Cable modems provide Internet access over cable TV networks (which use fiber-optic or coaxial cables). They are generally much faster than modems that use phone lines.
Cache	A copy of a program or data that is used for faster access. See also Web Cache.
Certificate Authority	An issuer of Security Certificates used in SSL connections. See also SSL.
Client	A computer system or process that requests a service from another computer system or process.
Data Encryption	Encrypting data is accomplished by applying a scrambling code that makes the data unreadable to anyone who does not have a decryption key. Authorized personnel with access to this key can unscramble it. Data encryption is a useful tool against malicious users.

DHCP	Dynamic Host Configuration Protocol This is an industry-standard protocol that assigns IP information to computers.
DNS	Domain Name System A set of guidelines and rules that allows you to navigate the Internet using domain names instead of IP addresses.
DDNS	Dynamic Domain Name System A system that automatically updates DNS information when a new IP address is assigned to a network.
DNS Server	A computer or server that matches an IP addresses to a domain name. Some ISPs provide a specific DNS address.
DSL	Digital Subscriber Line
Ethernet	A LAN that connects devices like computers, printers, and terminals. Ethernet transmits data over twisted-pair or coaxial cables at 10 or 100 Mbps.
EtherTalk	Networking protocol used by Apple equipment connected directly to Ethernet.
FastForward	The ability to create a passage (or open a port) through your firewall to a service or a server hosting a service. See also Port Number.
Firewall	A device that provides secure Internet access and protects internal networks from intruders.
FTP	File Transfer Protocol An Internet based protocol used to copy files between computers (usually a client and a server) using Unix-based command parameters. You can download shareware or freeware applications that remove all the complexities of Unix and allow you to connect to FTP sites using a web browser.

Gateway	A computer or server that is connected to multiple networks and is capable of routing or delivering packets between them.
HTML	Hypertext Markup Language A set of tags and instructions used to create web pages. HTML tags create page layouts, format text, insert graphics and multimedia, and more.
HTTP	Hypertext Transfer Protocol A protocol that makes hypertext information such as web pages available over the Internet.
Hub	A a piece of hardware that connects computers together in a LAN, allowing information to travel between them.
Internet Gateway	A gateway for accessing the Internet, which is loosely defined as points of entrance to and exit from a communications network. A gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture. A gateway can be thought of as a function within a system that enables communications with the outside world.
IMAP	Internet Message Access Protocol A popular protocol that allows a client to access email without downloading it to a local computer. Used mainly to read email from a remote location.
IMAP Server	A server that uses IMAP to provide access to multiple server-side folders.
IP Address	Internet Protocol Address The numeric address used to identify and locate a server, computer, or website on the Internet.
IP Address (Dynamic)	A temporary IP address that is assigned to a computer by a DHCP server each time it goes online.

IP Address (Static)	A permanent IP address that is assigned to a computer in a TCP/IP network. Network devices that serve multiple users (such as servers, routers, and printers) are usually assigned static IP addresses.
IPsec	Internet Protocol Secure A type of secure connection between computers at different locations, creating Virtual Private Networks. See also VPN (Virtual Private Network).
ISDN	Integrated Services Digital Networking A digital-communication networking system used for high-speed communication with the Internet. ISDN is available through most telephone companies.
ISP	Internet Service Provider An organization that maintains a server directly connected to the Internet. Users who are not directly connected to the Internet typically connect through an ISP.
Java	Designed by Sun Microsystems, Java is a programming language for adding animation and other action to web sites. In order to view web sites created with Java, your browser has to have Java enabled.
JavaScript	Designed by Sun Microsystems and Netscape as an easy-to-use supplement to Java, JavaScript code can be added to standard HTML pages to create interactive documents. Most modern browsers support JavaScript.
kbps	Kilobits per Second (thousands of bits per second) This is a measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium.
LDAP	Lightweight Directory Access Protocol The LDAP server provides a directory of users' names and email addresses.

LAN	Local Area Network A LAN links together computers that are in the same building. 10BaseT Ethernet is the most common LAN. See also Hub.
Mbps	Megabits per Second (millions of bits per second) This is a measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium.
MX Record	Mail Exchange Record A DNS resource record type that indicates which host can handle mail for a particular domain.
NetBIOS	Network Basic Input Output System. A protocol for networking on IBM PC and compatible systems.
NAT	Network Address Translation NAT allows one publicly visible IP address to refer to many IP addresses internally on a LAN, making it look like all traffic was generated by a single external IP address.
NFS	Network File System A protocol developed by Sun Microsystems which allows a computer to access files over a network as if they were on its local drive.
NIC	Network Interface Card An adapter card that physically connects a computer to a network cable.
Packet	A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.
Packet Filter	A filter that blocks traffic based on a specific IP address or type of application (email, FTP, web, etc.), which is specified by port number.

Peer-to-Peer Network	A network where there is no dedicated server. Computers with access privileges can share files and peripherals with all other computers on the network.
PhpMyAdmin	PHP <i>MySQL</i> Administration A program used to administer <i>MySQL</i> databases, and provides a user interface.
PING	Packet InterNet Groper A program used to determine if a server is functional. It sends small packets to the server, which replies with similar packets.
POP3	Post Office Protocol 3 A popular protocol used most often by ISPs for receiving email messages. POP3 servers allow access to a single Inbox (as opposed to IMAP servers, which provide access to multiple server-side folders).
Port Number	A number assigned to an application program running on a computer in a TCP/IP-based network such as the Internet. The number is used to link the incoming data to the correct service. There are several standard port numbers. For example, port 80 is used for web traffic.
PPP	Point-to-Point Protocol A method of transmitting protocols (such as IP) over a serial link. PPP is most often used in dial-up modem connections from a home computer to an ISP.
PPPoE	Point-to-Point Protocol over Ethernet PPPoE is often used to connect DSL providers. Because it is based on two common standards (PPP and Ethernet), it is easy to integrate into existing networks.
PPTP	Point-to-Point Tunneling Protocol PPTP ensures secure communications over Virtual Private Networks that use public phone lines.
Protocol	A set of rules that govern network exchanges.

Proxy Server	A server that acts as a barrier between an internal network and the Internet. Proxy servers can work with firewalls, which help keep outside users from gaining access to confidential information. A proxy server also allows the caching of web pages for quicker retrieval.
RBL	Realtime Blackhole List A ‘spam’ blocker that has different levels of spam protection (such as <i>Strong</i> or <i>Medium</i>).
Router	A device that handles the connection between two or more networks.
Routing	The act of directing packets between networks.
Routing Table	A list of destinations known to the router (server) that allows user traffic to get to and from its destinations.
RSA	Rivest Shamir Adleman An Internet encryption and authentication system that uses an algorithm developed by Rivest, Shamir, and Adleman.
Security Certificate	Information used by the SSL protocol to establish a secure connection. Contains information about who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted ‘fingerprint’ that is used to verify the contents of the certificate. See also SSL.
Server	A computer or software package that provides specific services to a client. The term can refer to a particular piece of software (such as a web server) or to the machine on which the software is running. A single server can run several different server software packages.
SNMP	Simple Network Management Protocol A protocol used to collect statistical information from a host about parameters such as central processing unit (CPU) utilization.

SMTP	Simple Mail Transfer Protocol A protocol used for transferring or sending email messages between servers. Another protocol (such as POP3) is used to retrieve the messages.
SQL	Structured Query Language A language used to create advanced databases.
SSL	Secure Sockets Layer A protocol that allows encrypted, authenticated communications to travel across the Internet. SSL is used mostly in communications between web browsers and web servers. URLs that begin with "https" indicate that an SSL connection is being used. Each side of an SSL connection must send a valid Security Certificate to the other. Each side then encrypts what it sends using both certificates, thereby ensuring that only the intended recipient can de-crypt it, that the other side can be sure of the data's origin, and that the message has not been tampered with.
Subnet	A portion of a network (which may be a physically independent network segment) that shares a network address with other portions of a network. A subnet is distinguished by its own subnet number.
TCP/IP	Transmission Control Protocol/Internet Protocol A popular suite of protocols that allow computers to communicate on the Internet.
Telnet	An application that lets you access resources on a Unix or Linux computer. In order to use Telnet, you need to be familiar with Unix-based programs.
UDP	User Datagram Protocol A protocol used throughout the Internet for services such as DNS.
URL	Uniform Resource Locator The standard method to give an address of any resource on the Internet. A URL looks like this: http://www.net-itech.com.

VPN	Virtual Private Network VPNs allow communication between users in different offices. To prevent people on the Internet from intercepting transmissions, all information that passes through a VPN is protected with 128-bit encryption, the strongest encryption technology available.
WAN	Wide Area Network A network that connects different LANs using routers.
Web Browser	An interface that lets you view material on the Internet. The most popular web browsers are from Microsoft and Netscape.
Web Cache	An area on your hard disk that is reserved for storing images, text, and other files that have been viewed on the Internet.
WebConfig	Net Integrator has a web-based configuration system. To connect to WebConfig, enter <code>http://hostname:8042</code> in the address bar of a web browser. For example, if your Net Integrator's host name is <i>thunder</i>, enter <code>http://thunder:8042</code> in the address bar. See <i>Chapter 2: Connecting to WebConfig</i> for more information.
WebMail Server	A system that allows users to access their email account using any standard web browser.

A

- address book, WebMail 120
- administrator account
 - creating 35
- anonymous FTP server 151
- Apache Public License 289
- Artistic License 283
- Automated Drive Mapping 89

B

- Backup 153
- BSD License 293

C

- calendar, WebMail 122
- components of, Net Integrator 11
- configuration of, Net Integrator 45
- Configuring 154

D

- data backup
 - idb (intelligent disk backup) 153
 - tape 153
- data restore
 - idb (intelligent disk backup) 158
 - tape 174
- DHCP server 22
- disk management 235
 - disk configuration 235
 - disk recovery 241
 - hard disk failure 241
 - idb 235
 - installing a new hard drive 242
 - RAID 235
 - reconfiguration of disks 236
 - status messages 238
 - SystemER 241
- DNS 213
 - domain registrars 215
 - dynamic DNS 216
 - entries, manual creation of 216
 - entries, types of 217
 - hierarchy 215
 - lookup and caching server 213
 - mail records 103
 - publishing server 213

- working with SMTP server 103
- Domain Controller 79
- domain names 46, 215, 217
- domain registrars, DNS 215
- DoubleVision 59
- DSL connection 57
 - configuration of 57
- dynamic IP addresses 228
- dynamic web site 256

E

- Email Aliases 99
- email services 95
 - advanced email settings 106
 - DNS mail records 103
 - IMAP server 97
 - LDAP server 98, 107
 - mail virus scanner 96
 - POP3 server 97
 - realtime blackhole list 96
 - SMTP server 96
 - WebMail server 97
- ethernet 16
 - cables 16
 - port connections 17

F

- FastForward 225
 - common port numbers 232
 - configuration of 229
 - creating a new forward 229
 - editing a forward 230
 - firewall security 225
 - proxy servers 227
 - static and dynamic IP addresses 228
 - TCP 227
 - TCP/IP 225
 - UDP 226
- file sharing services 77
 - configuration of 77
 - Macintosh file server 78
 - NFS file server 78
 - Windows file server 78
- file transfer protocol (FTP) 46
 - port 21 232
- firewall services 209

- log 211
- restrict outgoing traffic 209
- white paper 209

First 11

FTP services 149

- anonymous FTP server 151
- enabling FTP access 151
- enabling FTP server 151

G

GNU General Public License 265

GNU Lesser General Public License 273

H

hard disk failure 241

- installing a new hard drive 242

host names 46

hosting multiple web sites 135

I

idb (intelligent disk backup) 153

- initiating a backup 157

idb (intelligent disk backup) configuration 154

idb (intelligent disk backup) restore

- initiating a restore 158
- restore scenarios 158

idb Hot Swap 162

IMAP server 95, 104, 105

Import Users from Windows 65

installing new hard drive 242

intelligent disk backup (idb) 153

internet connections

- configuring a dial-up modem 55
- configuring a DSL connection 57
- configuring a leased line connection 58

IP address

- manually setting 21
- static and dynamic IP addresses 228

IPsec 189

L

LDAP server 107

- configuration of 107

leased line connection

- configuration of 58

Licensing 271

- log messages 257
 - customizing message display 258
 - firewall log 211
- Logon Scripts 88

M

- Macintosh file server 78
- mail virus scanner 96
- main status screen 40
- master web server 129
- MySQL server 247
 - Microsoft Access 252
 - phpMyAdmin 247

N

- network address translation (NAT) 183
- network devices 48
 - reconfiguration of 49
- network file system (NFS) 261, 273, 283, 287, 289, 291, 293
 - mounting an NFS directory 262
 - ugidd 261
 - unmounting an NFS Directory 262
- network routes 50
 - reconfiguration of 50
- network settings (advanced) 47
- network settings (general) 45
 - domain names 46
 - host names 46
 - public DNS server 46
 - rsync 46
 - SNMP 46
 - time setting 47
- NFS file server 78

O

- Operating Conditions 1

P

- Perl script 129
- PHP License 291
- PHP script 129
- phpMyAdmin 247
 - managing databases 248
- POP3
 - configuration of 97
 - mailboxes 61, 62

- server 95, 104, 105
- port numbers (common) 232
- positive web filtering 143
- power connection 15
 - power-up sequence 20
 - supply cord 11
- PPTP 197
- print services 91
 - configuring your workstation 91
- proxy servers 227
- public DNS server 46

R

- RAID 235
 - creating a RAID array 36
- realtime blackhole list (RBL) 96
- remote access services 197
 - dial-in connection 204
 - dial-in service 204
 - VPN connection 198
 - VPN service 197
- Replace Security Certificate 136
- Restore 158
- restrict outgoing traffic 209
- rsync 263

S

- secure web services 136
- setup, first-time 11
- shutdown button 238
- simple network management protocol
 - SNMP 46
- Smarthost 95, 98
- SMTP server 95, 105, 216
 - configuration of 96
- software update 177
- SSL Certificate 136
- SSL encryption 136
- static IP addresses 228
- SystemER 241
 - hard disk failure 241
 - installing a new hard drive 242

T

- tape backup 153
 - backup procedure 170

- initiating a backup 170
- tape restore 174
 - initiating a restore 175
 - restore scenarios 174
- TCP/IP workstation configuration 24
 - for Mac OS 9 32
 - for Mac OS X 34
 - for Windows 2000/XP 28
 - for Windows 95/98/ME 24
- team accounts 61, 70
 - creation of 71
 - deletion of 75
 - editing 74
 - service integration 61
- time setting 47
- transport control protocol (TCP) 227
- TunnelVision 181
 - configuring a client 186
 - configuring a master server 185
 - creating a VPN 184
 - encryption 182
 - idle time-out 187
 - network address translation 183
 - private networks 181
 - status 187
 - steel pipe 183
 - subnet numbers 184
 - VPNs 181

U

- user accounts 61
 - creating 62
 - deleting 65
 - editing 64
 - service integration 61
- user datagram protocol (UDP) 226

V

- views of, Net Integrator
 - back 14
 - front 12
- virtual network computing (VNC) 222
 - configuration of 222
- virtual private networks (VPNs) 181
- virtual web servers 133
- virus scanner

mail 96

W

- web caching 141
- web filtering 143
 - accepting access requests 145
 - adding permitted web sites 145
 - enabling 143
 - full Internet access 144
 - positive web filtering 143
- web services 129
 - hosting multiple web sites 135
 - master web server 129
 - secure web services 136
 - SSL encryption 136
 - virtual web servers 133
 - web server 129
 - webmaster directory 130
- WebConfig 23
 - configuring TCP/IP 24
 - creating an administrator account 35
 - main status screen 40
- WebMail 111
 - access to 113
 - address book 120
 - calendar 122
 - configuration of 116
 - email composition 117
 - opening email 118
 - replying to email 119
 - screen 114
 - server 95
- webmaster directory 130
- Windows file server 78
- workstation viewer 221
 - virtual network computing 222

X

X.509 Certificate 136

Z

Zlib License 287



Exchangel!

Usage Guide

INTRODUCTION	2
What is ExchangeIt!?	2
Outlook + ExchangeIt! - What do they do?	2
Purpose Of This Manual	3
INSTALLATION	4
Installing ExchangeIt!	4
SETTING UP YOUR OUTLOOK CLIENT	4
Configuring Microsoft Outlook 2000	4
Configuring E-mail	4
Directory Services Setup	6
Configuring Microsoft Outlook 2002	7
Configuring E-mail	7
Directory Services Setup	8
Installing Client Plug-in	9
Configure Outlook to use ExchangeIt!	10
To Enable Synchronization	10
EXCHANGEIT OUTLOOK FEATURES	12
The Folder List	12
Folders Accessible From Outlook	13
IMAP Mail Folder	13
Personal Folders	13
Public Folders	14
Creating Folders	14
Personal Folders	14
Public Folders	15
Using your ExchangeIt! Calendar	16
Calendar	16
Create a Meeting Request Using Free/Busy	16
Receiving and Responding to a Meeting Request	18
Booking Resources	19
Viewing Someone Else's Folders	19
Giving Someone Else Access to Your Folders	19
To give someone permission to access your calendar in Outlook:	19
To modify a user's permissions:	21
To delete a user's permissions:	21
EXCHANGEIT! UNBOUND	22
Understanding the installation process	22
Access Control List and Permissions (ACL)	24
Synchronization	25
User Licenses	25
Sharing of your Personal Folders	26
Team Folders	27
Public Folders	27
Uninstalling	28
Calendars, Free/Busy, and Meeting Requests	29

INTRODUCTION

What is ExchangeIt!?

ExchangeIt! provides collaboration services running as a fully integrated service on the Net Integrator server. *ExchangeIt!* works seamlessly with Microsoft Outlook to help you create, organize and share information quickly and easily.

Thanks to its complete integration into the Net Integrator operating system (“NIOS”), *ExchangeIt!* is able to take full advantage of advanced NIOS technologies such as NetIntelligence, idb, and System ER. This makes *ExchangeIt!* an easy collaboration system to set up, maintain and backup.

Outlook + ExchangeIt! - What do they do?

In order for Outlook to work with *ExchangeIt!* a small Outlook plug-in, developed by Net Integration and available free of charge, needs to be installed on every workstation that requires *ExchangeIt!* functionality. (*ExchangeIt!* licenses is handled on the server).

When you use the Microsoft Outlook mail client with *ExchangeIt!*, the following features are added to its functionality:

- **Schedule Sharing:** Personal Outlook calendars can be shared with other *ExchangeIt!* users.
- **Group Schedules:** Shared calendars can be created for multiple users (or Net Integrator “teams”); each team member will have access to the shared calendar. These shared calendars are the equivalent of shared public resources, and can relate to people or to conference rooms and other meeting resources such as video projectors.
- **Meeting Invitations:** Users can schedule meetings with other users and also book conference rooms and other meeting resources. Invite users to meetings; when they accept, the event appears in their calendar. View the free/busy times for meeting invitees and resources when scheduling a meeting.
- **Contact List Sharing:** Share personal contact lists with other users.
- **Group Contact Lists:** Maintain shared contact lists that everyone can access and contribute to.
- **Task List Sharing:** Share personal task lists with other users.
- **Group Task Lists:** Maintain shared task lists that all users or team members can contribute to.
- **Journal Sharing:** Share personal Outlook journals with other users.
- **Notes Sharing:** Share Outlook notes with other users.
- **Group Notes Sharing:** Maintain shared notes folders that all users or team members can access and contribute to.
- **Access Control Lists and Shared Folder Permissions:** Give other users or teams permission to view, edit or change calendars, contact lists, notes, journals and task lists. Each user or team can have “Read,” “Read/Write” or “Read/Write/Admin” rights to a folder.

- **Outlook Synchronization:** Information contained within Outlook personal folders (with the exception of deleted items and email messages) is uploaded and synchronized with the *ExchangeIt!* database. This yields the following advantages:
 - Backup – if a workstation’s Outlook data is lost, it can easily be re-synchronized from the server. The *ExchangeIt!* database is also backed up by the idb backup system on the Net Integrator server.
 - RoamingAccess – Outlook will have your synchronized personal folders even if you are on a different computer.
 - WebAccess – *ExchangeIt!* data is synchronized with the Net Integrator. WebMail web-based mail and collaboration interface. This allows easy access to a user’s Outlook data from any browser.
- NOTE: This feature is NOT available in the *ExchangeIt!* 1.0 release, but will be available in a future release.

NOTE: *ExchangeIt!* requires Microsoft Outlook 2000 or Microsoft Outlook 2002 running on a Windows 2000 or Windows XP platform.

Purpose Of This Manual

This manual will focus on the use of Outlook 2000 and Outlook 2002 with *ExchangeIt!*

Please refer to your Microsoft Outlook manual for the Outlook specific functionalities not covered in this manual.

INSTALLATION

Installing ExchangeIt!

See your System Administrator or Net Integrator representative for an *ExchangeIt!* client.

SETTING UP YOUR OUTLOOK CLIENT

Please Note: In order to use *ExchangeIt!*, you must have a user account on the Net Integrator.

Software Requirements: *ExchangeIt!* requires Microsoft Outlook 2000 or Microsoft Outlook 2002 running on a Windows 2000 or Windows XP platform. *ExchangeIt!* is not compatible with any version of Microsoft Outlook Express, Microsoft Outlook 98 or other mail packages.

Configuring Microsoft Outlook 2000

Please Note: For Microsoft Outlook 2002, see “Configuring Microsoft Outlook 2002” below.

Please Note: You need to have Microsoft's Web Publishing Wizard installed in order for the free/busy services to work with Outlook 2000 on Windows 2000. If this has not already been installed on your computer you can download the installation file from: <http://www.microsoft.com/downloads/release.asp?ReleaseID=22658>

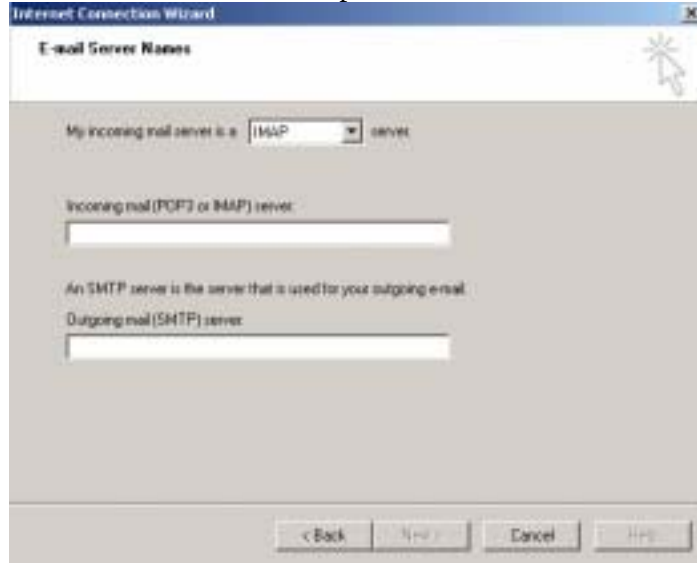
Configuring E-mail

If you are already using Outlook 2000 for your e-mail in *Internet mode*, select *Tools > Accounts*. Click on *Add > Mail*. The *Internet Connection Wizard* screen appears. Jump to Step five (5).

If this is your first time using Outlook 2000, start at step one (1).

1. Open Microsoft Outlook 2000.
Please Note: Corporate Mode Microsoft Outlook is not supported. Please go to *Tools > Options > Mail Delivery* and click on *Reconfigure Mail Support* to reconfigure Outlook to Internet Only mode. [If you are unsure how to accomplish this, please refer to your Office 2000 documentation].
2. The *User Name* screen appears.
3. Enter your *Name* and *Initials*. Click the *OK* button.
4. The *Internet Connection Wizard* screen appears.
5. Enter your *Display name* (this is the name that will appear on your outgoing e-mail). Click the *Next* button.
6. Enter your *E-mail Address*. Click the *Next* button.

7. The next screen will ask, “My incoming e-mail server is a ____ server.” Select *IMAP* from the server drop-down list.

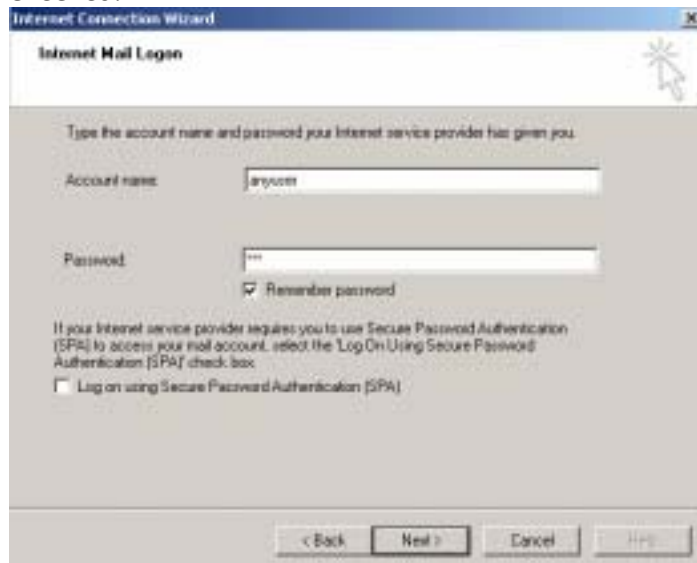


The screenshot shows the 'E-mail Server Names' window of the Internet Connection Wizard. It has a title bar with 'Internet Connection Wizard' and a close button. The window contains a section titled 'E-mail Server Names'. Below this, there is a label 'My incoming mail server is a' followed by a dropdown menu showing 'IMAP' and the word 'server'. Below that is a text box labeled 'Incoming mail (POP3 or IMAP) server:'. Further down is a text box labeled 'Outgoing mail (SMTP) server:'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Please Note: We recommend that you use an IMAP e-mail server. However, *ExchangeIt!* will work with POP3 e-mail servers, but you will lose your ability to have your mail remotely accessible.

8. Enter the name of your *incoming mail server* (this is the name of the Net Integrator).
9. Enter the name of your *outgoing mail server* (this is the name of the Net Integrator).
10. Click the *Next* button.
11. Enter your *Account name* and *Password* (password is optional).

Please Note: Ensure that the *Log on Secure Password Authentication (SPA)* is not checked.



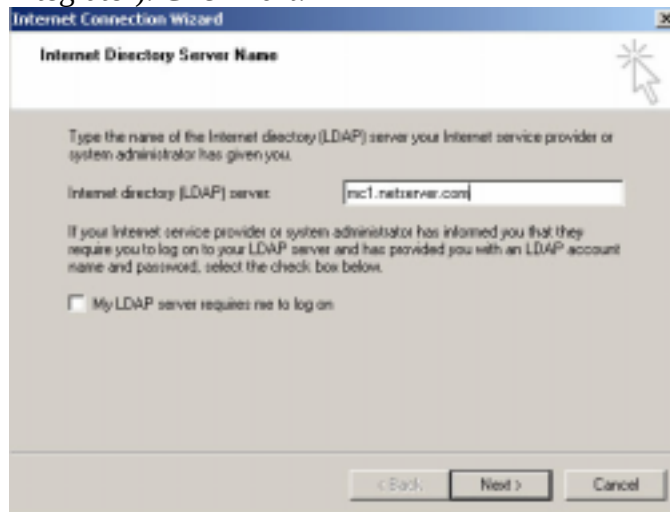
The screenshot shows the 'Internet Mail Login' window of the Internet Connection Wizard. It has a title bar with 'Internet Connection Wizard' and a close button. The window contains a section titled 'Internet Mail Login'. Below this, there is a label 'Type the account name and password your Internet service provider has given you.' Below that are two text boxes: 'Account name:' and 'Password:'. Below the password box is a checked checkbox labeled 'Remember password'. Further down is a text box labeled 'Log on using Secure Password Authentication (SPA)'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

12. Click the *Next* button.
13. Select which method you want to use to connect to the Internet (local area network).

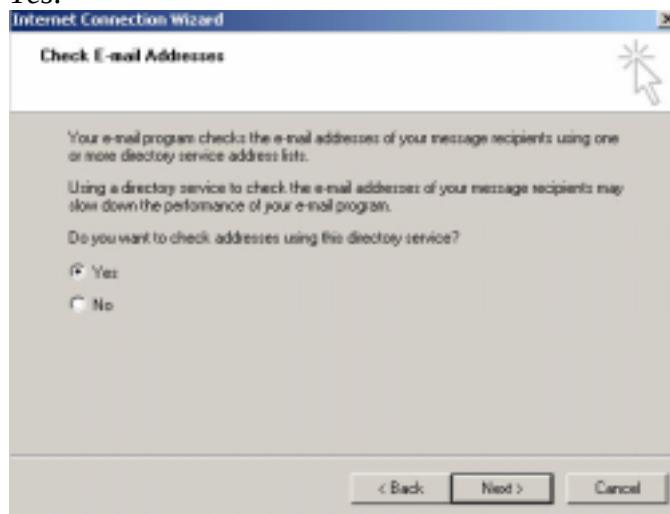
14. Click the *Next* button.
15. Click the *Finish* button.

Directory Services Setup

1. In Outlook, select *Tools > Accounts*.
2. Select *Add > Directory Services*.
3. The *Internet Connection Wizard* screen appears.
4. Enter your *Internet directory (LDAP) server* name (this is the name of the Net Integrator). Click *Next*.



5. It will ask, “Do you want to check Addresses using this directory service?” Select *Yes*.



6. Click the *Next* button.
7. Click the *Finish* button.
8. Click the *Close* button.
9. Close Outlook.

Configuring Microsoft Outlook 2002

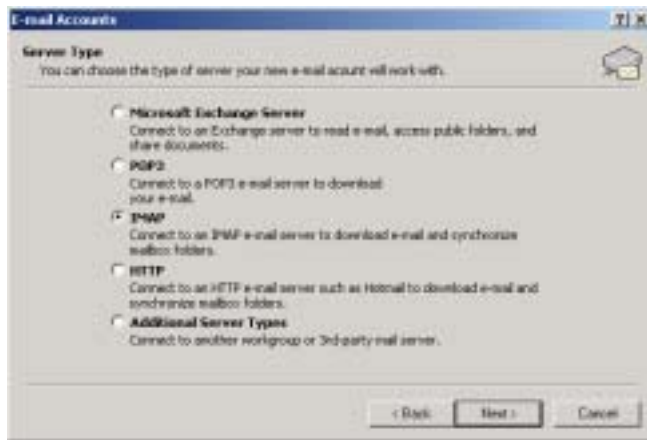
Please Note: For Microsoft Outlook 2000, see “Configuring Outlook 2000” above.

Configuring E-mail

If you are already using Outlook 2002, select *Tools > Accounts*, then click on *Add > Mail*. The *Internet Connection Wizard* screen appears. Jump to Step five (5).

If this is your first time using Outlook 2002, start at step one (1).

1. Open Microsoft Outlook 2002.
2. The *Outlook 2002 Startup* screen appears.
3. Click the *Next* button.
4. The *Account Configuration* screen appears.
5. Click the *Yes* button.
6. Click the *Next* button.
7. The *Email Accounts* screen appears asking you to select your e-mail server type. Select *IMAP*.



Please Note: We recommend that you use an IMAP e-mail server. However, *ExchangeIt!* will work with POP3 e-mail servers.

8. Click *Next*.
9. Enter your *User Information*, *Server Information* and *Logon Information*.



Please Note: Ensure that the *Log on Secure Password Authentication (SPA)* is not checked.

10. Click the *Next* button.

11. Click the *Finish* button.

12. The *User Name* screen appears. Enter your *Name* and *Initials*. Click the *OK* button.

Please Note: The *User Name* screen only appears if it your first time using Outlook.

Directory Services Setup

1. From Outlook, select *Tools > Email Accounts*.

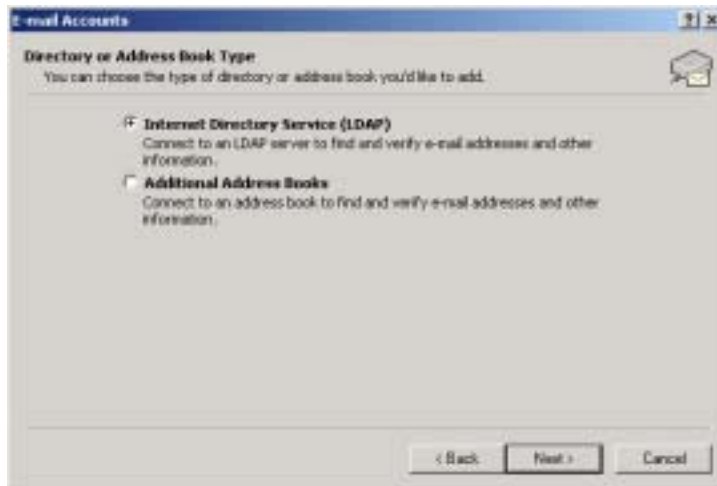
2. The *Email Accounts* screen appears.



3. Under *Directory*, choose *Add a new directory or address book*.

4. Click the *Next* button.

5. Select *Internet Directory Service (LDAP)*.



6. Click the *Next* button.
7. Enter the *Server* name.



8. Click the *Next* button.
9. The *Add Email Account* screen appears asking if it is okay to exit Outlook. Click the *OK* button.
10. Click the *Finish* button.

Installing Client Plug-in

Please Note: You must be logged in as the Administrator to install the *ExchangeIt!* plug-in. Installing the plug-in using a user account may not install the plug-in properly.

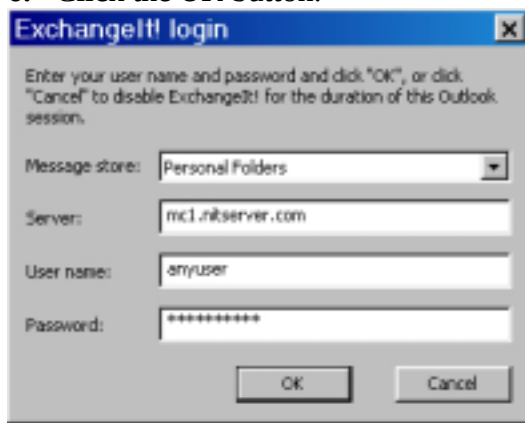
Please Note: You must configure Outlook before installing the *ExchangeIt!* plug-in.

1. Go to where you placed the *ExchangeIt!* plug-in.
2. Double-click the *ExchangeIt!* plug-in.

3. The *ExchangeIt! Plug-in for Microsoft Outlook Setup: License Agreement* window displays.
4. Click the *I Agree* button to accept license.
5. The *ExchangeIt! Plug-in for Microsoft Outlook Setup: Installation Folder* window displays.
6. Click the *Install* button to install the *ExchangeIt!* plug-in in the default destination, **or** select a different folder by using the *Browse* button then click on the *Install* button.
7. Once installation is complete, click the *Close* button.

Configure Outlook to use ExchangeIt!

1. Open Outlook.
2. The *ExchangeIt! Login* window displays:
3. Select the Message Store you wish to have synchronized. The default store is “Personal Folders.”
4. Enter the name of your Net Integrator *Server*. The default name is calendar.
5. Enter your *User name* and *Password*.
6. Click the *OK* button.



To Enable Synchronization

1. From the Outlook *Tools* menu, select *Options*.
2. Click on the *ExchangeIt!* tab.
3. Ensure that the *Enable ExchangeIt! periodic synchronization* is checked.



4. Click on the OK button.

EXCHANGEIT OUTLOOK FEATURES

The Folder List

Folders in Outlook can help you manage your mail by filing messages based on certain criteria that are at your discretion.

The folders within Outlook are used for storing items that you create in the various Outlook modules: e-mail messages, calendar items, contact names, tasks and sub-folders. Each module has its own folder that you can see in the Folder List. The Folder List is simply a list of the folders accessible from Outlook (see Figure 1).

For more details on these folders, see the next section, “Folders Accessible from Outlook”.

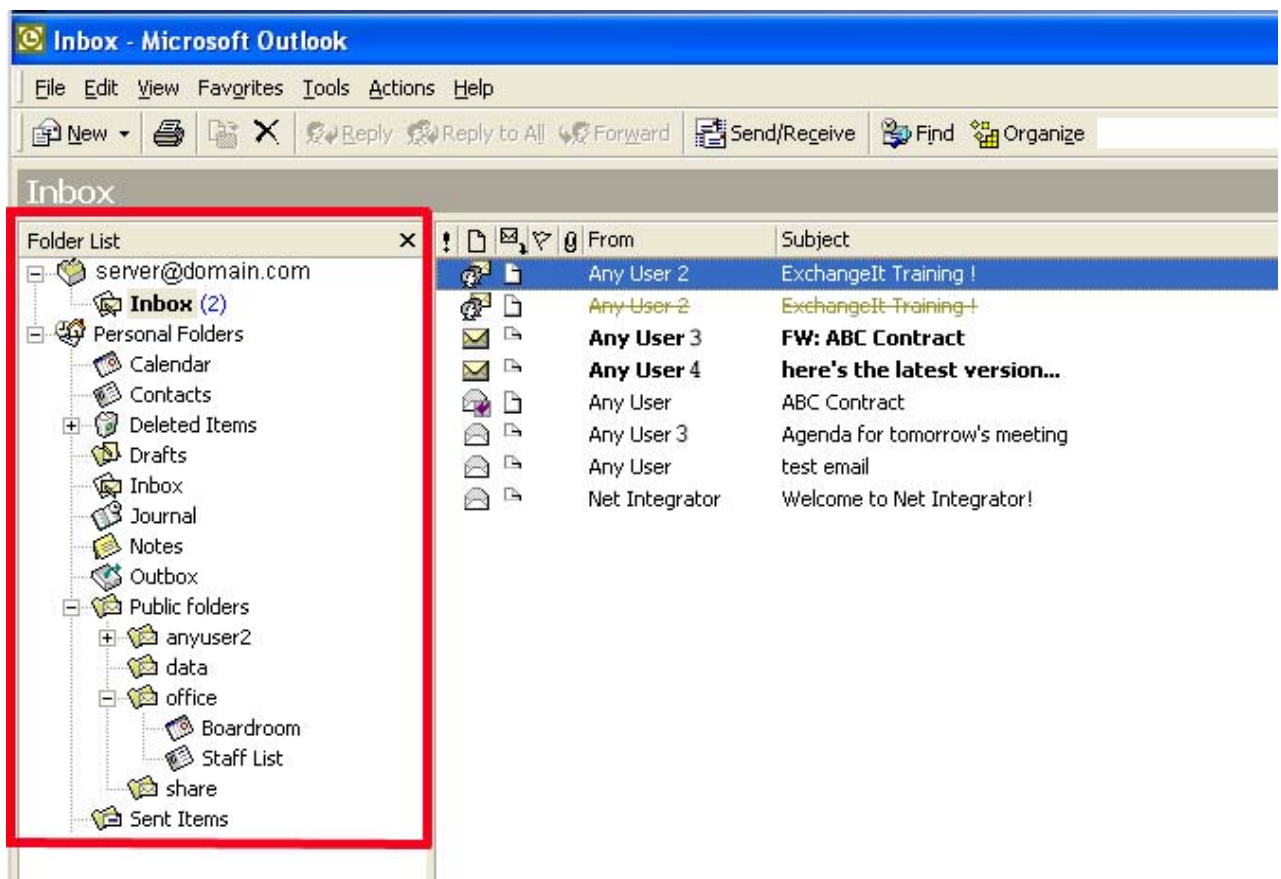


Figure 1

The Folder List in Outlook displays all of the folders that are located in your *ExchangeIt!* server account, Public Folders, as well as those located in your Personal Folders.

To see the Folder List select *View* from the Outlook toolbar and click on *Folder List*.

Folders Accessible From Outlook

The Folder List in Outlook will allow you to see all of the folders that Outlook can access. These folders can be stored on the *ExchangeIt!* server, your hard drive or a network share.

Outlook can access any folders and subfolders in your account on the *ExchangeIt!* server, as well as Public Folders. Folders not on the *ExchangeIt!* server that Outlook can access are your Personal Folders.

IMAP Mail Folder

The folder entitled *Inbox* under your server name (see Figure 2) in the Folder List view is the root folder in your account on the *ExchangeIt!* server.

IMPORTANT: When using Outlook with IMAP, your e-mail will be delivered to the *Inbox* under your server name, and not the *Inbox* under your *Personal Folders*.

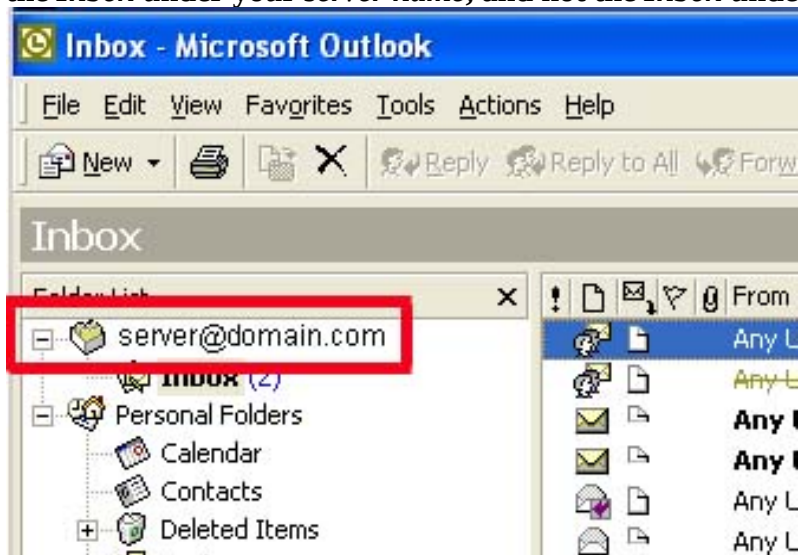


Figure 2

Personal Folders

The Calendar, Contacts, Deleted Items, Drafts, Inbox, Journal, Notes, Outbox, Sent Items and Tasks folders in the “*Outlook today - [Personal Folder]*” or “*Personal Folder*” folder are all subfolders of your Mailbox. (Note: you can create your own subfolders that will be stored on the *ExchangeIt!* server in your account – see Creating Folders).

ExchangeIt! enables you to share any of your Calendar, Contacts, Tasks, Notes or Journal files in your Personal Folders with other user(s). These shared folders are only open to

those who are given permission by the creator or the "owner" of the folder. (By default, no one but you has permission to access your Personal Folders).

Public Folders

Public folders (see Figure 3) are stored on the *ExchangeIt!* server and may not be particular to anyone's account. They serve as a location on the *ExchangeIt!* server for the files shared with you by other users and for files shared by members of a Net Integrator "team account." In Figure 3 for example, a Contacts list for office staff ("Staff List") was created in the team access folder entitled "office" under the Public Folders so that everyone in the office had permission to look at the contents of the folder.

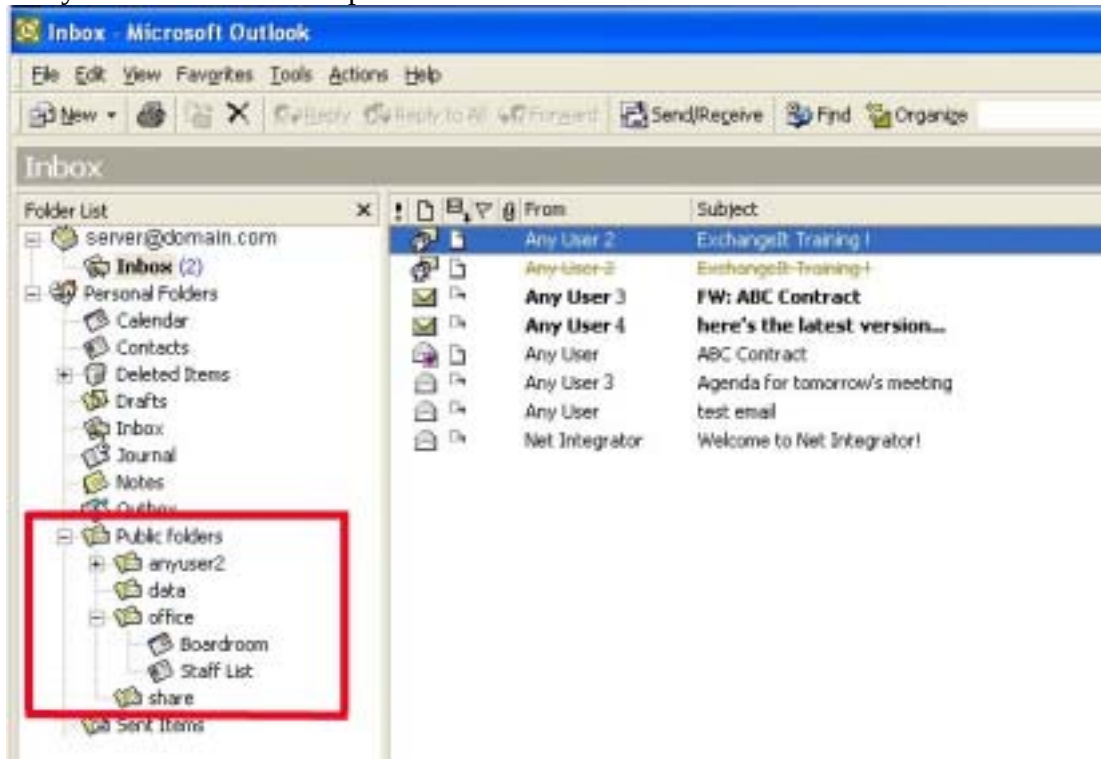


Figure 3

Creating Folders

Personal Folders

You can create new folders in your Personal Folders to share with other users.

1. Right click on *Personal Folders* (see Figure 4).
2. Enter a *Name* for the new folder.
3. Select the type of folder from the *Folder Contains* drop-down list (you can select Appointment, Contact, Journal, Mail, Note or Task Items). (Figure 4b).
4. Click *OK*.

NOTE: for information on sharing the new folder, see Giving Someone Else Access to Your Folders.



Figure 5



Figure 4b

Public Folders

You can create new folders in the Public Folders under team accounts.

1. Right click on the team account folder under *Public Folders* (see Figure 5).
2. Enter a *Name* for the new folder.
3. Select the type of folder from the *Folder Contains* drop-down list (you can select Appointment, Contact, Journal, Mail, Note or Task Items). (Figure 5b).
4. Click OK.

NOTE: for information on sharing the new folder, see Giving Someone Else Access to Your Folders.

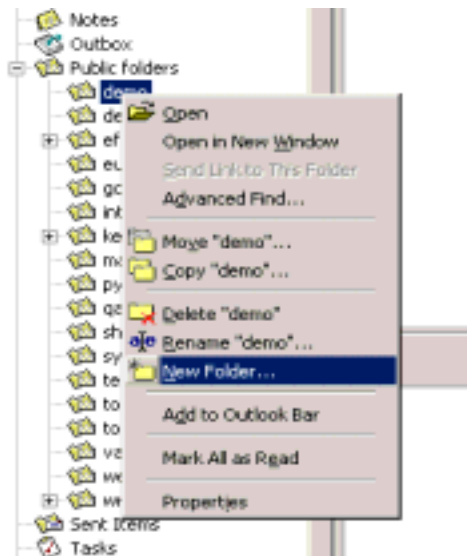


Figure 7

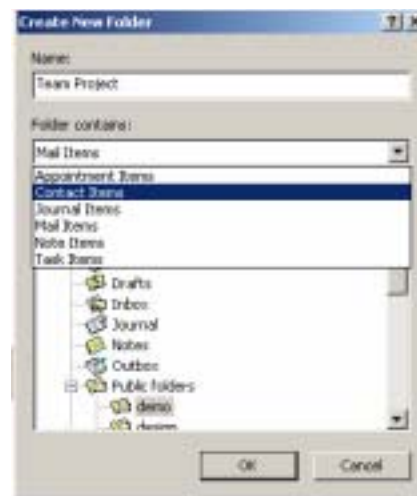


Figure 6b

Using your Exchange! Calendar

Calendar

The calendar folder allows you to keep track of your daily schedule as well as schedule meetings with others. Figure 6 is a screenshot of a typical calendar in daily view. This view allows you to see your schedule for a particular day, along with your Task pad. As you can see, you can create meetings and appointments with the Calendar folder.

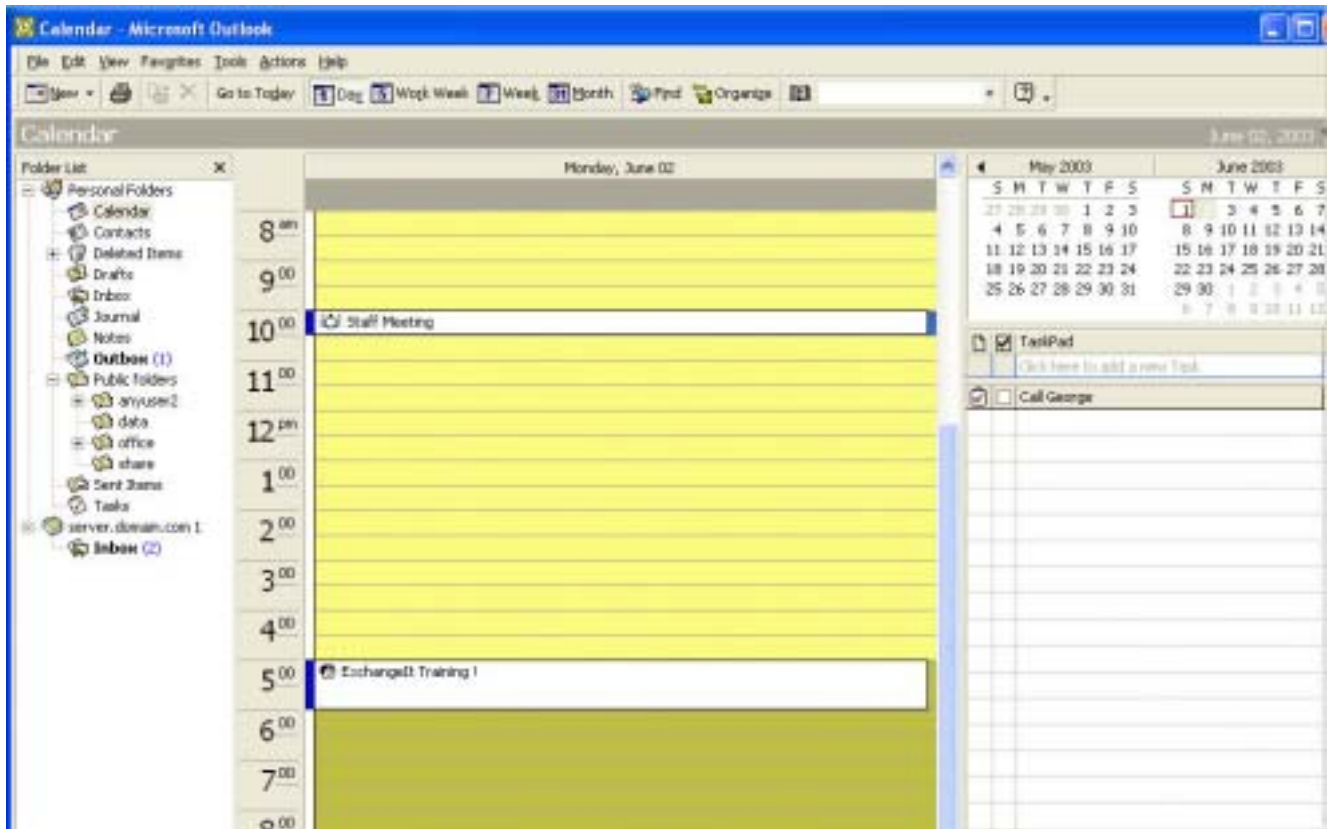


Figure 8

Create a Meeting Request Using Free/Busy

Please Note: You need to have Microsoft's Web Publishing Wizard installed in order for the free/busy services to work with Outlook 2000 on Windows 2000. If this has not already been installed on your computer you can download the installation file from: <http://www.microsoft.com/downloads/release.asp?ReleaseID=22658>

1. Click on the *Calendar* folder from the Folder List.
2. On the monthly calendar, double-click on the date on which the meeting is to occur.
3. An *Appointment Window* will appear (see Figure 7).

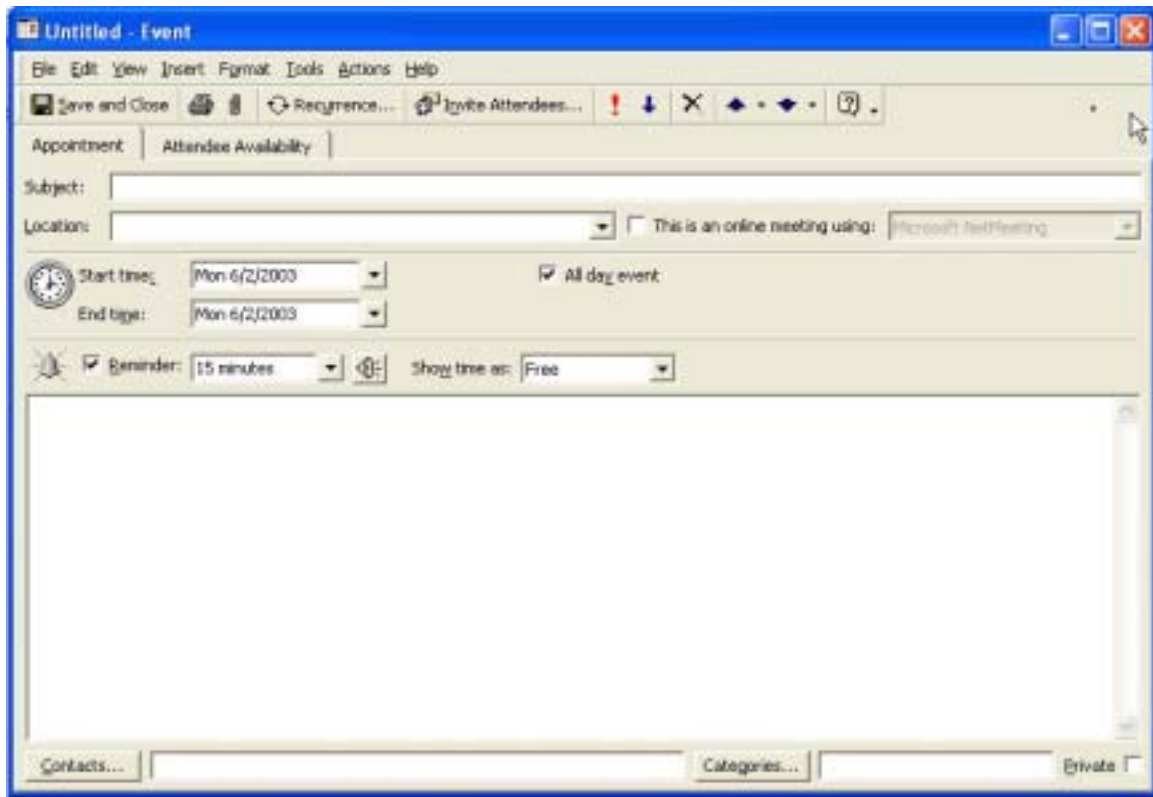


Figure 9

4. Enter the meeting date, start and end times in the bottom section. In the *Subject* field, enter the subject of the meeting. In the *Location* field, type the location of the meeting.
5. If desired, type additional information about the meeting in the text section. Attachments can be added in this field.
6. Click on the *Attendee Availability* tab.
7. Click on the *Invite Others...* button. Select the names of individuals who should attend the meeting.
NOTE: Names can be put in the *Required* or *Optional* attendee boxes.
8. Click *OK* when finished.
9. On the *Attendee Availability* screen, the attendees are listed on the left and their availability is shown in colored lines on the right. In Figure 8, 'AnyUser1' is free to attend the meeting at 11:00, but 'AnyUser2' is busy (blue) from 10:00 to 10:30.
NOTE: This is the only information that others will see on your calendar.

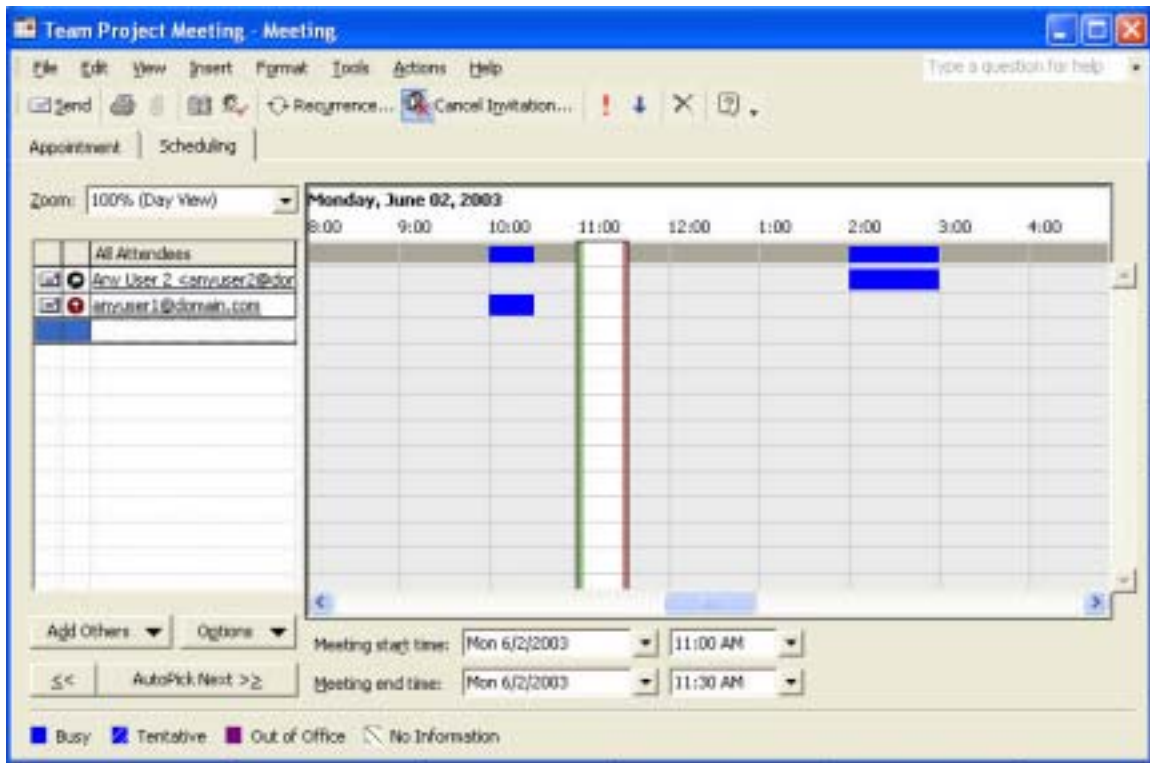


Figure 10

10. At this point, you can change the meeting date, start or end time depending on attendee availability.

NOTE: The AutoPick button to the left of the meeting times can be used to let Outlook select the next available time that all of the attendees have a free slot with enough time to schedule your meeting.

11. After completing the meeting request, click the *Send* button.
12. The meeting request is then e-mailed to all invited attendees. Invited attendees have the option of Accepting, Declining, or Tentatively Accepting the meeting invitation.

Receiving and Responding to a Meeting Request

Meeting requests are e-mailed to you from the requester. To reply to the meeting request:

1. Click the *Reply* button
2. Enter your response to the individual. You can choose to either Accept, Decline, or Tentatively Accept the meeting invitation.
3. Check the *Send the Response Now* option and click *OK*.

Meetings that are accepted are automatically entered onto an attendee's calendar.

Booking Resources

Outlook can be used for booking all kinds of resources, such as meeting rooms, projectors or whatever resources needs to be shared in your organization.

Simply create a new shared calendar folder under Public Folders and name it as the resource (i.e. Boardroom). In this calendar, you can view the resource's availability and reserve the resource for meetings or other events, thereby eliminating overlapping appointments. You can also "invite" this resource when creating a Meeting Request and the meeting will be entered into the resource's calendar.

NOTE: Someone must "own" the resource calendar in order to accept meeting requests; otherwise, the meeting will not be entered into the resource's calendar. The better alternative is to make the meeting request from the resource's calendar. This will automatically have the booking appear in the calendar of the resource.

Viewing Someone Else's Folders

In order to view someone else's folder that they have shared to you (i.e. calendar), the person must give you at least read-only permission. After they have given you permission, you will be able to see the folder and its contents. The folder will appear under Public Folders under the username of the person sharing the folder to you (Figure 9).

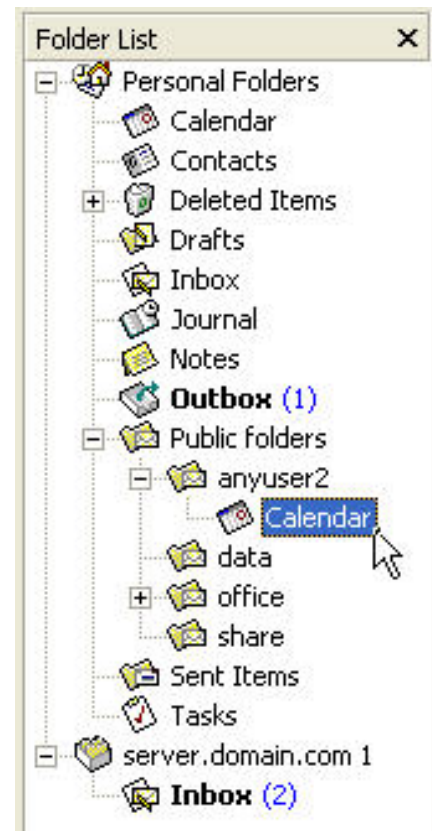


Figure 11

Giving Someone Else Access to Your Folders

To give someone permission to access your calendar in Outlook:

- Right-click on the folder you wish to share in your Folder List.
- Select the *Properties* option from the pop-up menu that will appear.
- When the *Properties* dialogue appears, select the *ExchangeIt! Permissions* tab. (You will now see the screen in Figure 10. This screen will show you the list of users and teams who are already authorized to access your calendar and their level of Permission).



Figure 12

- d. Click on the *Add* button. This will bring up the list of users and teams on your *ExchangeIt!* server (Figure 11).



Figure 13

- e. Select the user or team to whom you wish to give access this folder from the *Choose user* drop-down menu and click *OK*. You will be brought back to the screen shown in Figure 10.
- f. Click on the user or team that you've just added (make sure that the user or team is highlighted) and then assign them a *Permission level* from the *Permission level* drop-down list.
- g. Click *Apply*.
- h. Click *OK*.

To modify a user's permissions:

1. Right-click on the folder.
2. Select the *Properties* option from the pop-up menu that will appear.
3. When the *Properties* dialogue appears, select the *ExchangeIt! Permissions* tab. (You will now see the screen in Figure 10. This screen will show you the list of people who are already authorized to access your calendar and their level of permission).
4. Select the user or team that you want to change Permission level (make sure that the user or team is highlighted) and then assign them their new Permission level from the *Permission level* drop-down list. (Figure 12).

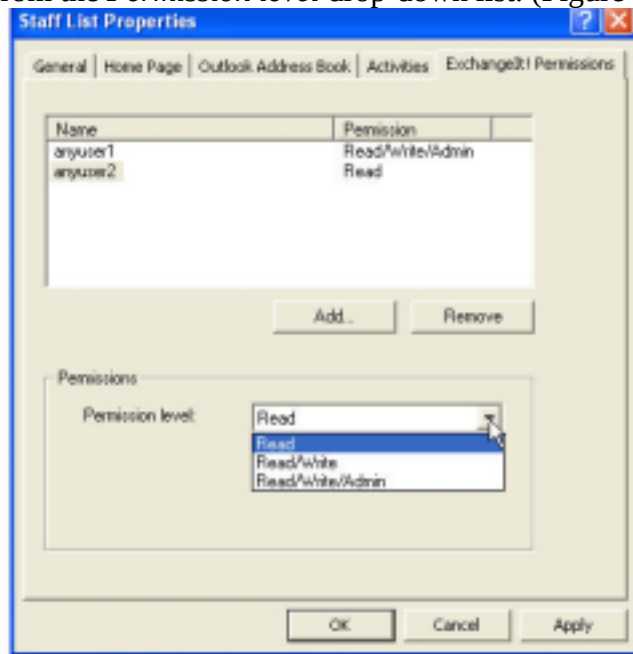


Figure 14

5. Click *Apply*.
6. Click *OK*.

To delete a user's permissions:

1. Right-click on the *Calendar* folder in your Folder List.
2. Select the *Properties* option from the pop-up menu that will appear.
3. When the *Properties* dialogue appears, select the *ExchangeIt! Permissions* tab. (You will now see the screen in Figure 10. This screen will show you the list of users and teams who are already authorized to access your calendar and their level of permission).
4. Select the user or team that you want to delete (make sure that the user or team name is highlighted).
5. Click on the *Remove* button.
6. Click *Apply*.
7. Click *OK*.

EXCHANGEIT! UNBOUND

This section of the guide is intended to give users and administrators additional insight into how *ExchangeIt!* and the Outlook plug-in work to allow for your items to be synchronized.

The Outlook plug-in client is required in order for Outlook to synchronize folders properly with the *ExchangeIt!* server. The plug-in enhances Outlook's native capabilities by communicating with the *ExchangeIt!* server to send and receive data corresponding to the folders and their contents based upon Access Control Lists (ACL). The ACL is used between the Outlook plug-in and the *ExchangeIt!* server to properly share the folders and their contents to other users.

It is probably best to understand the behaviour of the plug-in and how it interacts with Outlook to accomplish these tasks to allow you to best take advantage of *ExchangeIt!*'s capabilities.

Understanding the installation process

Installation of the plug-in is a straightforward process. However, it is recommended that the plug-in be installed using an administrative account because many workstations are deployed such that regular users are restricted from installing / uninstalling software.

To allow for multiple users to work on the same workstation, the plug-in creates separate profiles for each user based upon their Windows login. Once the plug-in installation has occurred, each time a new user logs onto Windows and opens Outlook (but has not previously configured the *ExchangeIt!* client) they will be asked to configure the client.

All the settings that are entered during this first time login may be later modified by selecting the *Tools* Menu of Outlook, then selecting *Options*. This will pop up a dialog box that has an *ExchangeIt!* tab. Selecting this tab will show the user the *ExchangeIt!* settings and allow the user to modify them.

There are 5 settings fields:

- a. Message Store
- b. Server
- c. User name
- d. Password
- e. Enable *ExchangeIt!* periodic synchronization (only appears if selected from the Outlook Tools -> *ExchangeIt!* dialog box)

Message Store

Outlook is capable of using multiple message stores. For most users, they will only have one open and available. The default Outlook message store is called “Personal Folders.” Some of the more advanced Outlook users may have multiple message stores. This field allows them to select the message stores that the *ExchangeIt!* plug-in is able to detect in Outlook based upon availability of folders that it can share such as Calendar and Tasks. For almost all users, selecting Personal Folders is best. Please refer to Microsoft Outlook’s documentation for further information on the use and setup of message stores.

The selection of the message store tells the plug-in that this is the message store for which the user will be synchronizing to the *ExchangeIt!* server.

Server

This field selects the *ExchangeIt!* server for which you wish to communicate with for synchronization. The default name is “calendar.” This is a private DNS entry set by the Net Integrator when *ExchangeIt!* is enabled. In most installation cases, this default name will be sufficient. However, if the workstation is not receiving its DNS from the Net Integrator running *ExchangeIt!*, the server name will need to be modified to the name being resolved by the local DNS server. Using the *ExchangeIt!* server’s IP address will also work, but if the local IP address of the server is dynamic, it may pose problems later if the IP address changes.

User name and password

The user needs to enter their username and password. This needs to be a valid account on the Net Integrator hosting the *ExchangeIt!* server. Although it is possible to modify the username after the initial installation, it is highly recommend that you don’t attempt to do so. If you wish to switch usernames, it is best to go through an uninstall and reinstall process rather than simply switching usernames, as many folders will be obsolete and other folders will appear with confusing results to Outlook.

Enable *ExchangeIt!* period synchronization

By default the periodic synchronization is enabled. Disabling this option will prevent the plug-in from communicating with the *ExchangeIt!* server. For the times that you may wish to disable the synchronization (i.e. working off-line), disabling this option will stop messages that may appear warning you that it is unable to communicate with the *ExchangeIt!* server.

Additionally, you will want to have this option disabled for users that you don’t wish to use *ExchangeIt!*. Disabling this option will prevent the plug-in from requesting the user information each time the user opens Outlook (if they aren’t utilizing *ExchangeIt!*), since clicking cancel at the request only disables the *ExchangeIt!* plug-in during that particular Outlook session.

Access Control List and Permissions (ACL)

The *ExchangeIt!* server provides access to items based upon permissions set on a folder-by-folder basis. In other words, the permissions of all items contained within a folder are based upon the permissions set on the folder itself.

The following describes the 3 permission levels and what they imply to the end-user with respect to the items within the folder and the folder itself.

Read-Only permissions

Items within the folder:

Users that have been granted read-only permissions to a folder are only allowed to view items in the folder. They do not have the ability to synchronize any modifications of items to the server. This means that the user can attempt to add, delete or edit the items, but all the modifications will be lost when the folder resynchronizes with the server, as the server will deny all changes forcing the plug-in to delete any additions, or edits, and retrieve the original (including items that were deleted).

The Folder:

Users that have been granted read-only permissions to a folder do not have the ability to synchronize the deletion of the folder or the creation of sub-folders. If the user attempts to delete the folder, the plug-in will retrieve the folder from the server during subsequent synchronizations. Any sub-folders that the user attempted to create will be deleted. Users are able to view the permissions set for the folder but will not be able to modify the ACL for that folder.

Read/Write permissions

Items within the folder:

Users that have been granted read/write permissions have the ability to read, add, delete and edit items within the folder. Any modification of the items within the folder will be synchronized with the server and then propagated to all other users that have permissions to the folder.

The folder:

Identical to the read-only permission level, users that have been granted read/write permissions to a folder do not have the ability to synchronize the deletion of the folder or the creation of sub-folders. If the user attempts to delete the folder, the plug-in will retrieve the folder from the server during subsequent synchronizations. Any sub-folders that the user attempted to create will be deleted. Users are able to view the permissions set for the folder but will not be able to modify the ACL for that folder.

Read/Write/Admin permissions

Items within the folder:

Users that have been granted read/write/admin permissions have the same capabilities as those with read/write permissions.

The folder:

Users that have been granted read/write/admin privileges have the ability to create and delete any sub-folders (unless they don't have read/write/admin privileges of the sub-folder they are attempting to delete), and the folder itself (only if they also have read/write/admin permissions to the parent folder). In addition to the ability to view ACL information for the folder, the user has the ability to make modifications to the ACL.

NOTE: Viewing of items marked "Private" requires Read/Write/Admin permissions.

If a user has administrative privileges on the Net Integrator itself, he/she will have read/write/admin permissions to all *ExchangeIt!* folders, whether or not they have been shared to that user.

Synchronization

The *ExchangeIt!* server and the Outlook plug-in work together to synchronize data between Outlook and the server. Unlike some other groupware/collaboration tools, the data is not accessed directly from the server. Instead, when the user edits, creates, deletes, or any way modifies the folders or folder contents, they are working with the data that is locally resident. This implies that at all times, there are at least two copies of the item (one locally, one on the server, and possible one or more to copies in other users' Outlooks) unless the item has not been synchronized yet. Using this approach has several benefits: The server has a copy that can now be automatically backed up by the Net Integrator; users are able to see and modify items off-line.

Because of the design, there are several important things to realize and keep in mind.

- a. Sharing of data is a two step process –
 - 1) Modifications to the folders and their contents first need to be synchronized between the server and the user that made the modification.
 - 2) The modification is synchronized between the server and the other users to whom the folder is shared with.
- b. Because the folder(s) and its contents are actually locally resident in Outlook and the server, modifications, copying and moving items is actually a "deletion" of the previous item(s) / folder(s), then the "creation" of the new item(s) / folder(s).
- c. If a user's permissions to see a folder is removed, this is treated as a delete by Outlook plug-in.

User Licenses

All licenses for *ExchangeIt!* are controlled on the *ExchangeIt!* server itself. Licenses are allocated per user. Each user that is licensed is allowed access the *ExchangeIt!* server from up to three simultaneous IP addresses. The IP addresses are tracked, aged, and

obsoleted automatically by the server. This allows each user the capability to simultaneously log in from different workstations, or to migrate from workstation to workstation. Thus remote users have the ability to work remotely on their laptop, yet still access the *ExchangeIt!* features when they use a desktop at the office.

The licenses can be assigned in two different ways. Users can be assigned a static *ExchangeIt!* license or have their license drawn from a pool of available dynamic licenses.

When users are assigned a license statically, their usernames will automatically appear in the ACL. Additionally, their license will not be redistributed to another user. Static license assignment and re-assignment must be done by the Net Integrator administrator using the Web Configuration.

If the user is to use a dynamic license, the user will only appear in the ACL after having recently connected to the *ExchangeIt!* server. Thus, if you have more users than you have licenses, it is still possible to utilize *ExchangeIt!*, but you must manually track who's accessing *ExchangeIt!*, otherwise, users may at some point not be able to access and synchronize anymore because not enough licenses are available.

It is recommended that the licenses be allocated statically as this will avoid confusion should there be more users than there are licenses available, and it will also avoid confusion in the ACL when user names don't appear and disappear.

Sharing of your Personal Folders

All folders originating from a user's message store will automatically be shared and synchronized to the server with read/write/admin privileges to the user themselves. This allows for the user to migrate to different workstations and have full access to their Personal Folder contents (except mail). If the user wishes to share the contents to other users, they must explicitly do so by modifying the ACL (by right-clicking on the folder and selecting the *ExchangeIt!* tab). Remember that ALL of the folder's contents are shared (except mail), so make sure there aren't items in there you do not wish to share prior to setting the ACL.

It is possible to create sub-folders and share the sub-folders without sharing the contents of the parent folder. For example, it is possible to create a sub-folder within "Contacts" called "shared." In addition to having contacts within the parent "Contacts" folder, you can have contacts also in the "shared" folder. You can choose to share the "shared" folder and not share the contents of the "Contacts" folder. Other users will see that "shared" has a parent folder called "Contacts," but they will not have the ability to look at the ACL or see the contacts contained within it.

Team Folders

Team and Public Folders

With the integration of *ExchangeIt!* into the core of the Net Integrator, users are able to take advantage of Net Integrator's team accounts.

Team folders work like any other folder – the only difference is that the team members are automatically granted full read/write/admin privileges to the team folders. Using team folders is one way for team members to work collaboratively by creating sub-folders containing tasks, notes, or any of the other shareable content without having to have someone designated as “hosting” the team's data. The team folders will be synchronized to each of the team members utilizing *ExchangeIt!*.

It is also possible to create sub-folders for a team that you can share to other users or teams. This is useful for allowing other teams or users access to certain contents without allowing them access to everything. For example, you can create a team on the Net Integrator called “facilities” with only a few members on that team. Create a calendar sub-folder called to “facilities” called “main boardroom” with read-only permissions granted to everyone. This allows you to have members of the team “facilities” administer the bookings for the “main boardroom.” Thus everybody will have the ability to see when the “main boardroom” is in use, while only members of “facility will be able to modify.” Of course this is just one specific example, you can setup the permissions and teams in a multitude of ways to handle proper administration and access to company resources.

Teams and the ACL

The concept of teams can also help to facilitate sharing of folders and the setting of permissions. In the ACL, all teams will appear. You can set the ACL permissions any combination of users and teams. Setting the permission level for a team implies that everyone that is a member of that team is granted that permission level. If a particular folder is shared to users and/or multiple teams, the recipient user gains the highest permission level combination.

For example – if there is a team with everyone in the company called “everyone,” and another team called “finance,” you can choose to share your contacts at read-only permission level to “everyone” AND share it with read/write privileges to “finance.” So even though members of the “finance” are also members of “everyone,” they will have read/write permissions while everybody else has read-only permissions.

Public Folders

If a user has folders that they have shared to them – a new parent folder will appear called “Public Folders.” Beneath this “Public Folders” will appear with one or more sub-folders listed by the source. The source name is either the Team name or the username of the user from whom the folder is being shared.

Creating folders directly under Public Folders

The only way to create folders directly beneath “Public Folders” is:

- a. another user shares one or more of their personal folder(s) with you
- b. being a member of a team
- c. another team has shared one or more folders with you

Although it may appear that users are able to create folders that are directly parented by “Public Folders,” this is in fact not possible. When the plug-in resynchronizes with the ExchangeIt! server, all “created” folders and any content will be removed (read deleted) by the plug-in.

Deleting folders directly under Public Folders

Your ability to delete folders is dictated by the permissions you have been granted by the ACL. Because no one has permissions at the “Public Folders” level (by design), you will not be able to completely remove folders directly parented by “Public Folders”.

Remember that to delete the folder itself you need to have read/write/admin privileges to the folder as well as to the parent.

If the user deletes a folder for which they have read-only permissions, the folder and all of its contents will be restored when the user is resynchronized.

If the user deletes a folder for which they have read/write permissions, the folder will be restored, but all the contents will be deleted when the user is resynchronized.

If the user deletes a folder for which they have read/write/admin permissions, the folder will be restored, but all the contents as well as any sub-folders for which they have read/write/admin privileges will be deleted.

Notice that these permission levels will be obeyed by all subfolders as well. Thus a deletion will force a deletion of all contents and sub-folders to maximum extent possible given the permissions of the user deleting.

Uninstalling

Exiting Outlook and then running the uninstall from the “Add/Remove programs” of Windows will uninstall the *ExchangeIt!* plug-in.

Because of the design of *ExchangeIt!* to work locally with Outlook, all the Public Folders that have been shared with the user will still be present in Outlook. The user will need to open Outlook and manually delete the Public Folders to get rid of all the content.

For a “clean” re-install of the plug-in, the following steps should be taken:

- 1) Exit Outlook
- 2) Uninstall the plug-in
- 3) Open Outlook and delete “Public Folders”
- 4) Exit Outlook
- 5) Re-install the plug-in

Calendars, Free/Busy, and Meeting Requests

Outlook is mostly capable of using standard formats for the updating and requesting of other Outlook users' free/busy information and booking of meetings. This allows people to book meetings with other users (or resources), and instantly see when people (or resources) are available.

ExchangeIt! extends this capability by providing a locally hosted free/busy server. Without the locally hosted free/busy server, users wishing to utilize this feature would have to send their information to one of the Internet hosted servers. Using an Internet hosted server can bring a host of potential problems.

The plug-in utilizes Outlook's native capability to talk to a free/busy server by automatically filling in the appropriate address tag in the Free/Busy options during installation.

ExchangeIt! and the Outlook plug-in utilize standard protocol and standard formats for the transport of data and communications between Outlook and the *ExchangeIt!* server. Because of these standard implementations, there are a few things that the system administrator and the users need to know and understand.

Most of the functionality utilized is native to Outlook. Unfortunately, Outlook doesn't handle some of the standards very well.

Meeting Requests

In particular, Outlook has problems with the receiving of meeting requests from Internet standard "iCalendar" meeting requests. Note that these are issues with Microsoft Outlook and not due to the installation of the *ExchangeIt!* plugin. The presence of the plug-in does not alter this behaviour. These are some known issues with Outlook (see references below for more information).

The work-arounds that we recommend for the sending of meeting requests (so they can be received properly) are as follows:

A) If everybody is using Windows and Microsoft Outlook:

- 1) From Outlook's Tools Menu: Preferences Tab-> Calendar Options
Disable the "when sending meeting requests over the Internet, use the icalendar format.
- 2) From Outlook's Tools Menu: Mail Format Tab
"Compose in this message format:" should be selected to "Rich Text"
- 3) From Outlook's Tools Menu: Mail Format Tab -> Internet Format
"When sending Outlook Rich Text messages to Internet recipients, use this format:" should be selected to "Send using Outlook Rich Text format"

B) If there is a mixture of Outlook 2000 and Outlook 2002 and other clients, there will be some incompatibilities. To reduce these incompatibilities we suggest the following when you are creating the meeting request:

- 1) Do not enable the “reminder”.
- 2)
 - i) In the “To” box, type the recipient’s e-mail address, and then double-click the e-mail address.
 - ii) In the E-mail Properties dialog box, in the Internet format box, change the option from “Let Outlook decide the best sending format” to “Send Plain Text only.”

<http://support.microsoft.com/default.aspx?scid=kb;en-us;218376>
<http://support.microsoft.com/default.aspx?scid=kb;en-us;284392>
<http://support.microsoft.com/default.aspx?scid=kb;en-us;307313>