NET INTEGRATION TECHNOLOGIES INC.

NET INTEGRATOR

User Manual

Version 3.71

This device complies with CAN/CSA-C22.2 No.950-95, UL 1950 Third Edition, and IEC 950 (1991).

This device also complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: *This equipment has been tested and found to comply with the limits for a Class B digital devices, 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 instruction manual, 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 of 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.

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

Publication Date: December, 2002

Chapter 1

First-time Setup

Net Integrator Technical Support

Net Integration Technologies' toll-free technical support line:

1-86-NET-ITECH (1-866-384-8324)
Outside of North America call **905-946-1777, ext. 400**
Hours of operation: 8:30 am to 5:30 pm EST, Monday to Friday

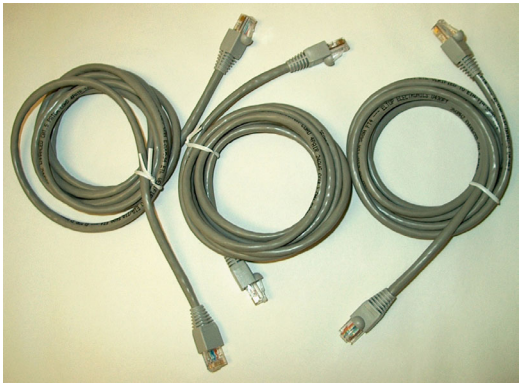
Email support questions to support@net-itech.com.

Net Integrator Components

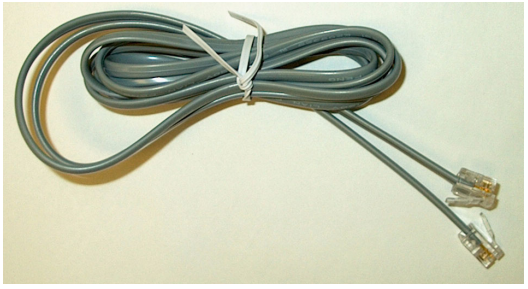
You should have received the following components in your Net Integrator package (photos are not to scale):

1. Net Integrator Server (1)
2. Net Integrator User Manual (1)
3. Quick Start Guide (1)
4. Hard Disk Keys (2)
5. Power supply cord (1)

6. 10baseT cables (3)



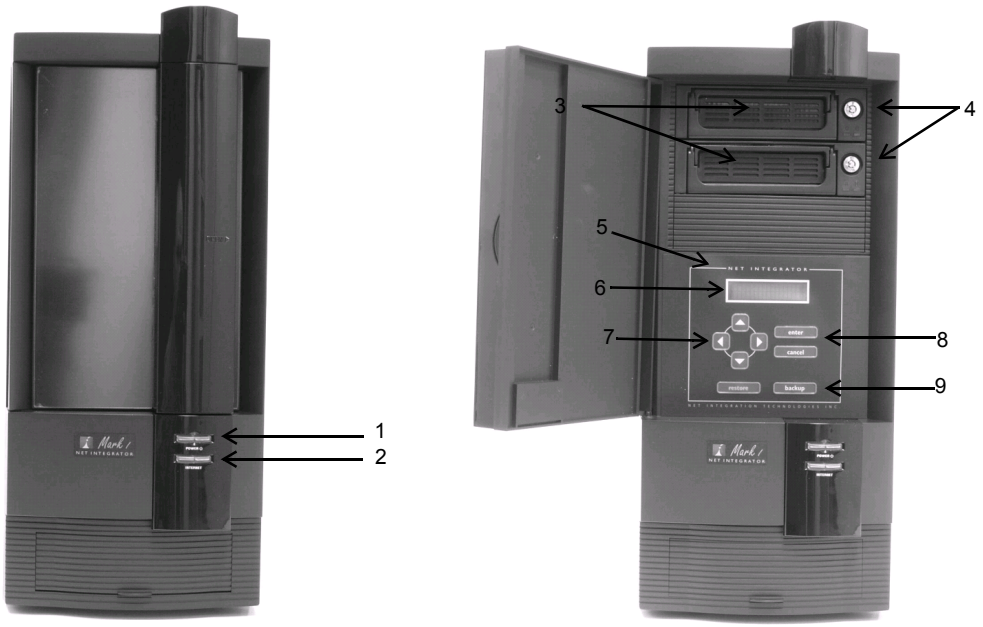
7. Modem cable (1) (Optional)



Meet Your Net Integrator

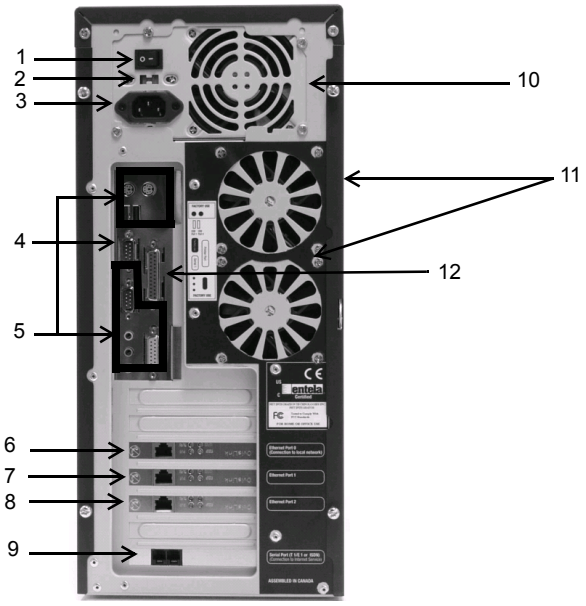
Front View

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.



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 tray(s)** – houses the hard disk(s).
4. **Hard disk key lock** – locks the hard disk in place.
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.

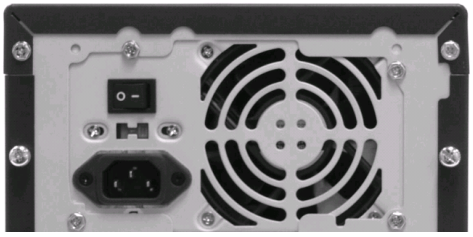
Back View



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.
2. **AC power selector** – indicates the voltage used in your country.
3. **Power socket** – where the power cord is connected.
4. **Serial port** – for an external dial-up modem.
5. **Extra ports** – 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. **Dial-up modem port** – used to connect to the Internet using a dial-up modem. (Optional)
10. **Power supply fan** – provides cooling for internal components.
11. **Primary and secondary cooling fans** – provides additional cooling for internal components.
12. **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:



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: 10base2 and 10baseT/100baseT. Networks generally use one or the other, although it is possible to combine them in certain situations.

Net Integrator can connect with either10baseT cables (which transmit data at 10 Mbps) or with 100baseT cables (which transmit data at 100 Mbps). Because 10baseT and 100baseT cables are faster and more reliable than 10base2 cables, we suggest that you use either of these to set up your local area network (LAN). 10baseT and 100baseT Hubs

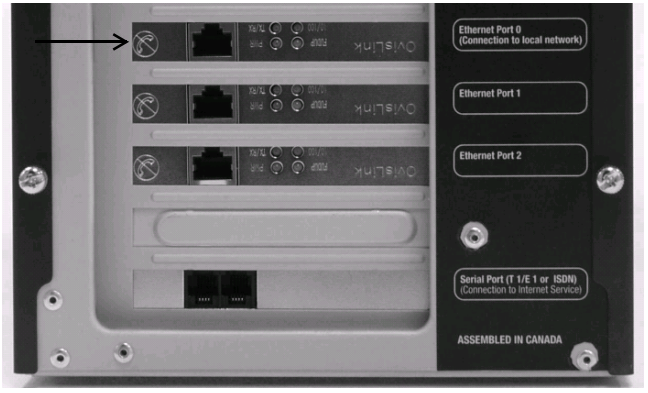
10base T and 100baseT hubs have a number of ports that you connect to a workstation, router, server, printer, or other device using an ethernet cable (which is similar to a phone cable). Connect your Net Integrator to a free port using one of the 10baseT cables that came

with your Net Integrator. If the port lights up after you connect and then turn on your Net Integrator, you have a proper connection.

You can attach another hub to one of the ports, thereby increasing the total number of ports (although we recommend that you consult the manual that comes with your hub before trying this).

Connecting Ethernet Port 0

1. Connect one end of a 10BaseT ethernet cable into *Ethernet Port 0* (located on the back of your Net Integrator).

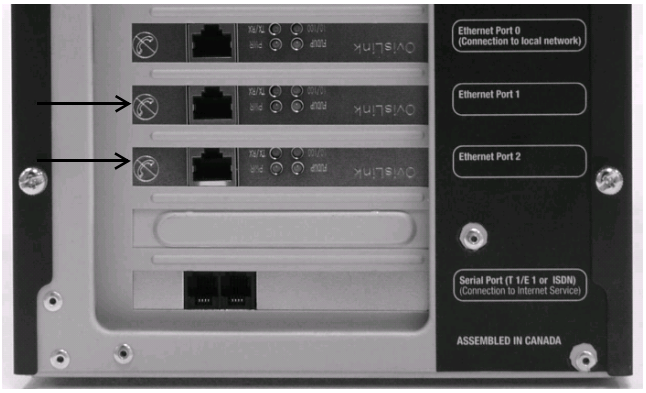


2. Connect the other end of the cable into your LAN hub or switch.

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. Please consult with your IT specialists for maximum security/configurability.

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 a 10baseT ethernet cable if you are connecting to a high-speed Internet connection with a router, cable modem, or DSL modem. Some DSL and cable modems require standard cables. In this case, use the cable provided to you by your ISP.



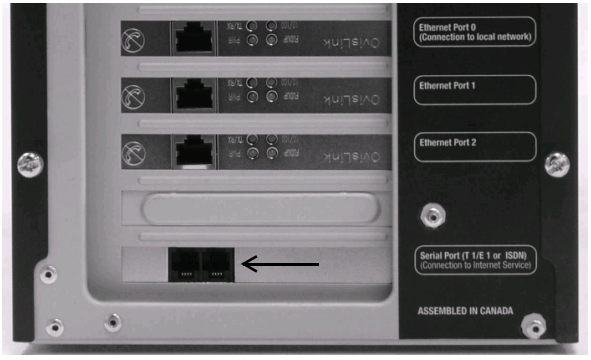
If you are using your Net Integrator as a workgroup server without a direct connection to the Internet, it is possible to use Ethernet ports 1 and 2 to connect to other segments of the LAN. This is typically done to improve network throughputs when large numbers of users are connected to Net Integrator.

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 Internal Dial-up Modem

(Optional)

1. Connect one end of a standard telephone cable into the *Analog Modem (Line)* port on the back of your Net Integrator.



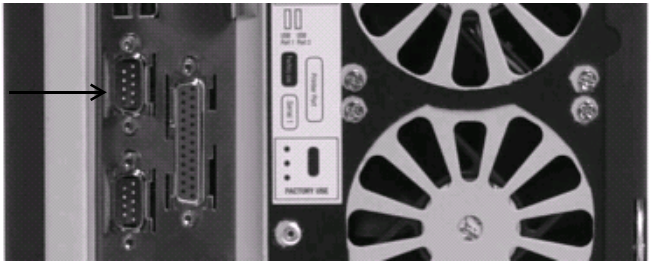
2. Connect the other end of the cable to your telephone wall jack.

   Please Note: Make sure that your telephone jack provides a standard analog telephone line. Net Integrator cannot connect to digital lines provided by some PBX telephone systems.

Connecting an External Dial-up Modem

(Optional)

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 (on the back of your Net Integrator).
2. Press the *Power* button.

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 discovery is being performed appear on the display panel. After about 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 operat-

ing 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.

Chapter 2

Connecting to WebConfig

What is WebConfig?

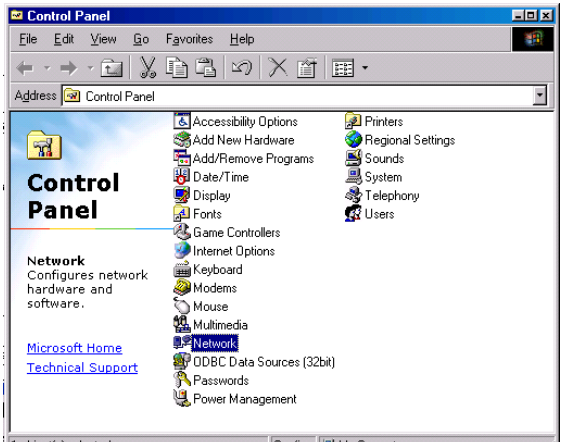
Although some basic system configuration can be done through the front control panel, the web-based configuration system (WebConfig) is where you will set most Net Integrator options.

Configuring TCP/IP

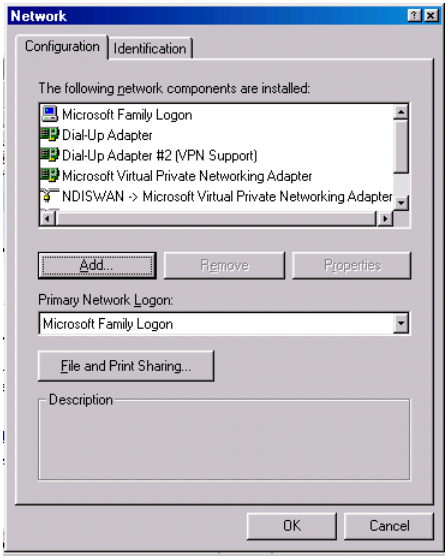
Before you can access WebConfig, you have to configure your workstation to use TCP/IP. If TCP/IP is already configured, proceed to *Creating an Administrator Account* (later in this chapter). If TCP/IP is not configured, follow the appropriate steps for your operating system.

For Windows 95/98/ME:

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

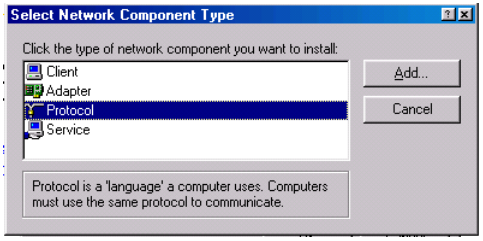


2. Select *Network* from the list. The *Network* window displays:



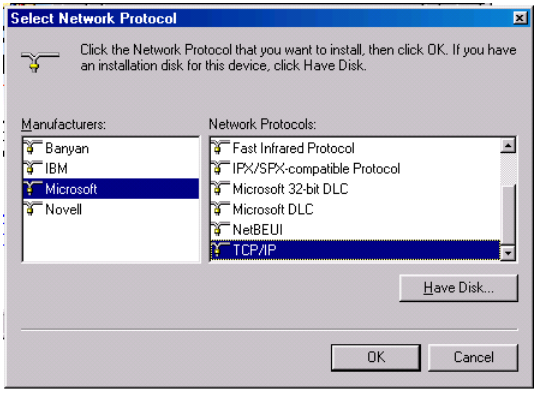
Click on the *Add* button if TCP/IP does not display in the installed components list.

3. The *Select Network Component* window displays:

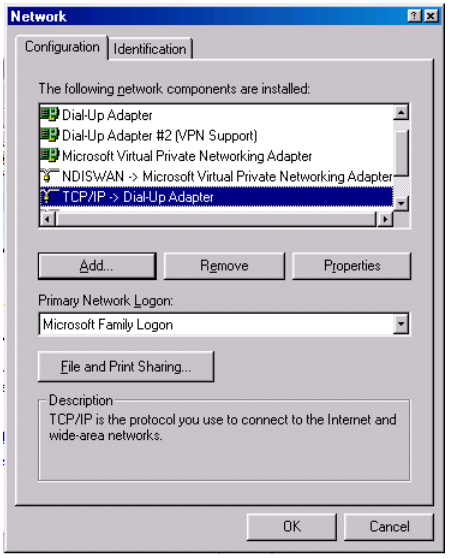


Select *Protocol* from the window. Click *Add*.

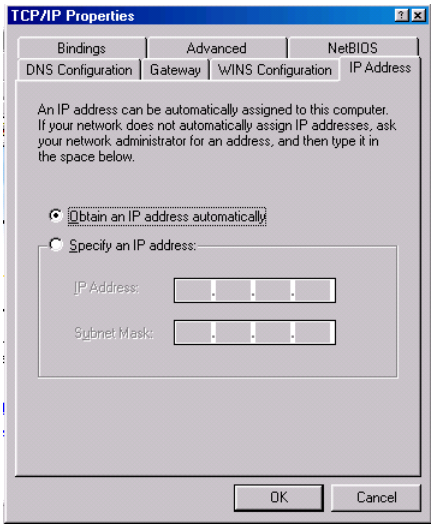
4. The *Select Network Protocol* window displays:



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.



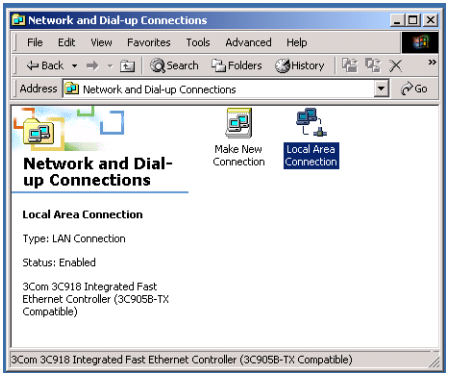
5. Select *TCP/IP* from the installed components list on the *Network* window. Click on the *Properties* button. The *TCP/IP Properties* window displays:



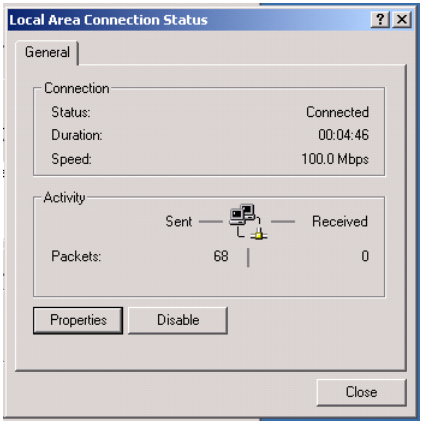
6. Click on the *IP Address* tab. Select *Obtain an IP address automatically.*
7. Click on the *DNS* tab. Select *Enable DNS.*
8. Select all entries in the *DNS Server Search Order* section of the window and click on the *Remove* button.
9. Select all entries in the *Domain Suffix Search Order* section 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:

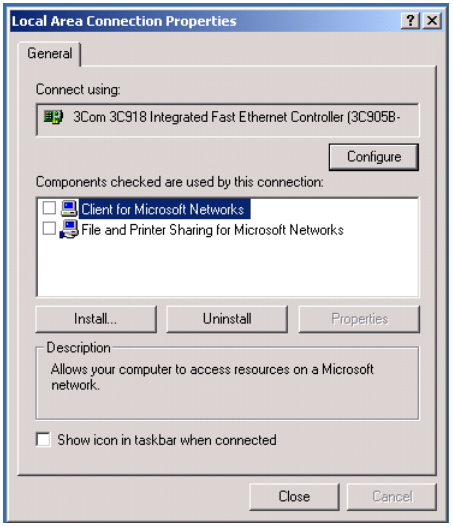


3. Click on *Local Area Connection*. The *Local Area Connection* window displays:



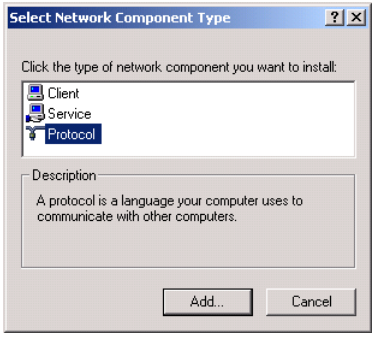
Click on *Properties*.

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



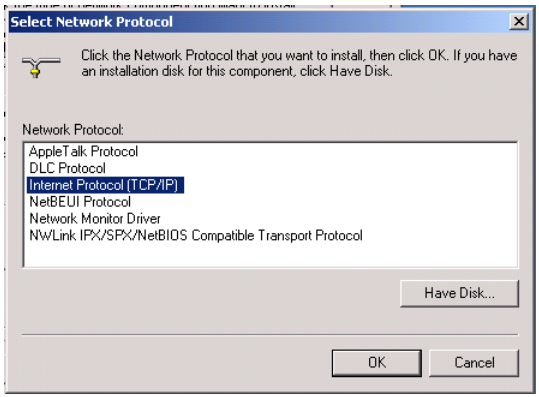
If *Internet Protocol (TCP/IP)* is not in the *This connection uses the following items* list, click on *Install*.

5. The *Select Network Component Type* displays:

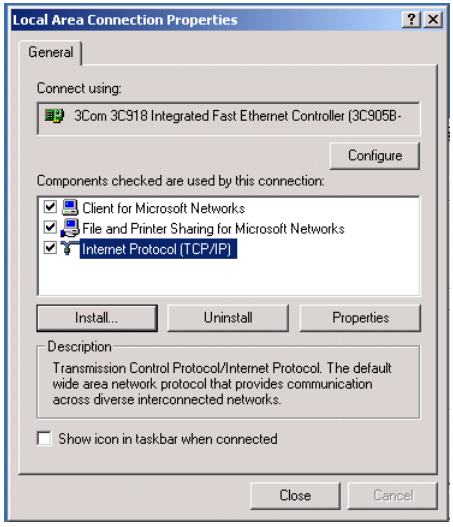


Select *Protocol* from the window. Click on *Add*.

6. The *Select Protocol* window displays:

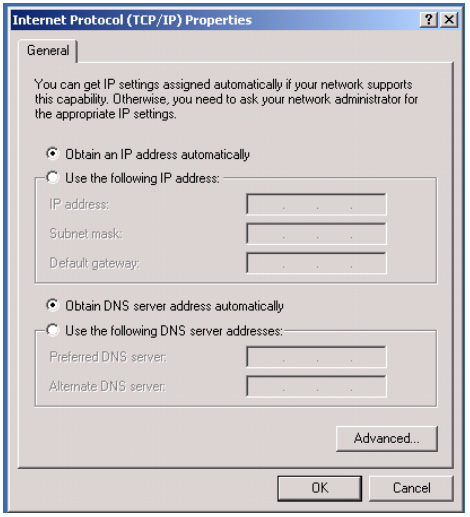


Select *Internet Protocol (TCP/IP)* from the list. Click *OK*. TCP/IP should now display on the *Local Area Connection Properties* window.



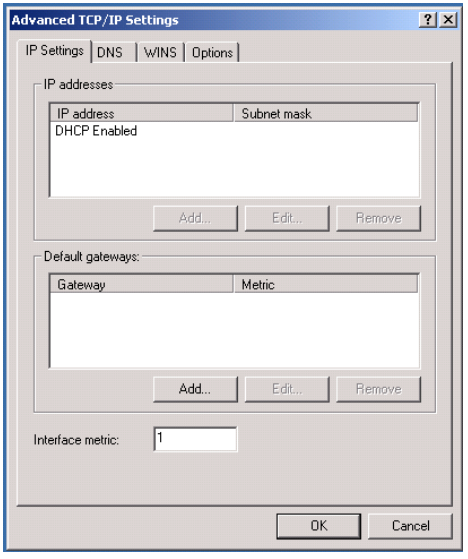
7. Select *Internet Protocol (TCP/IP)* from the list, and click on the *Properties* button.

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:

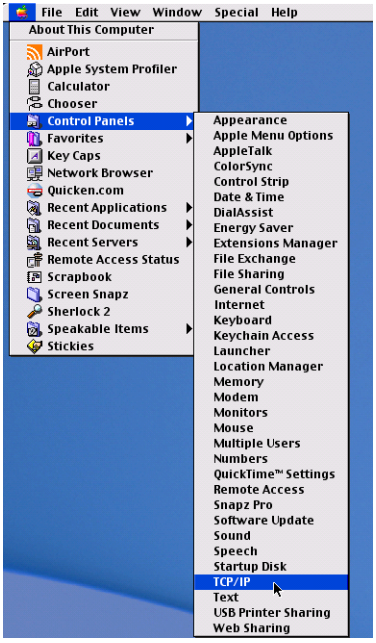


Select any entries in the *Default gateways* section of the window, and click on the *Remove* button.

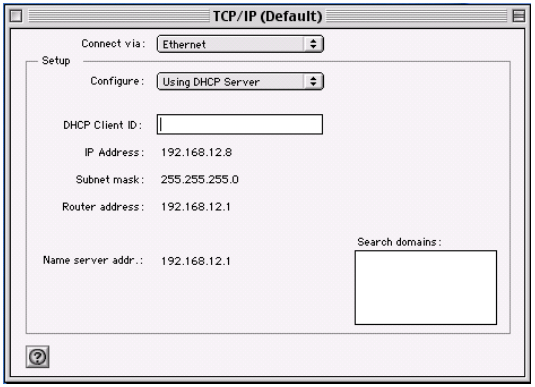
10. Click on the *DNS* tab. Select any entries in the *DNS server addresses* section of the window, and click on *Remove*. Select *Append primary and connection specific DNS suffixes*. Select *Append parent suffixes and primary DNS suffixes*.
11. Click on the *WINS* tab. Select any entries in the *WINS 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:

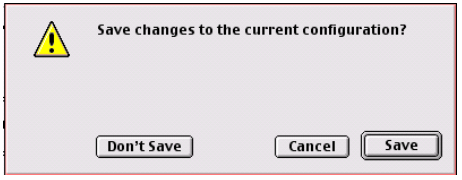
1. Click on the *Apple* icon in the top menu bar. Select *Control Panel* > *TCP/IP*.



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:

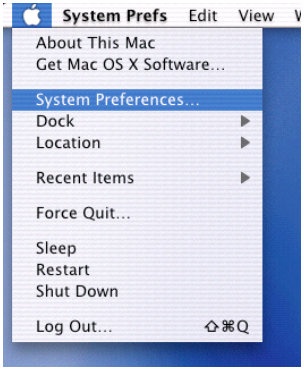


Click on *Save*.

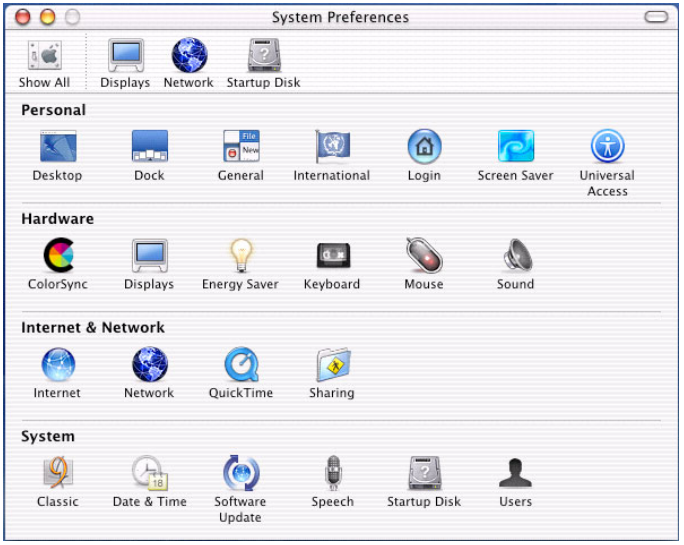
4. If the Internet connection doesn't function immediately, reboot your computer.

For Mac OS X:

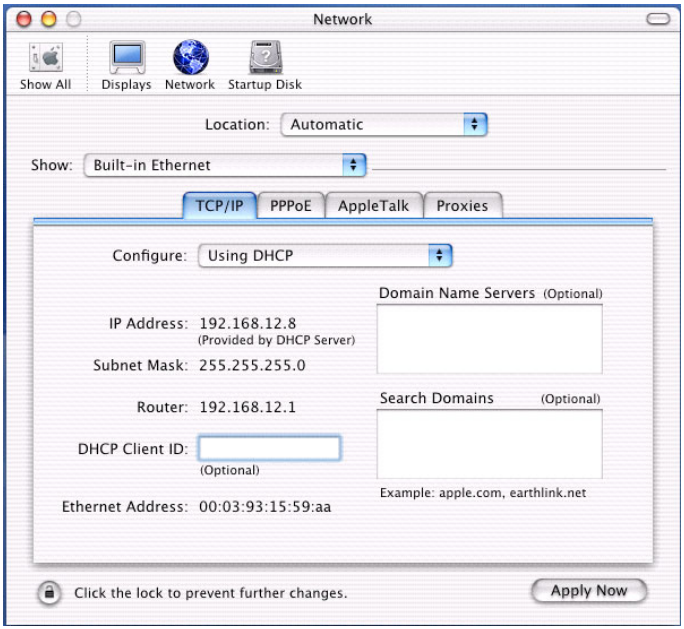
1. Click on the *Apple* icon in the top menu bar. Select *Control Panel* > *System Preferences*.



The *System Preferences* window displays:



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



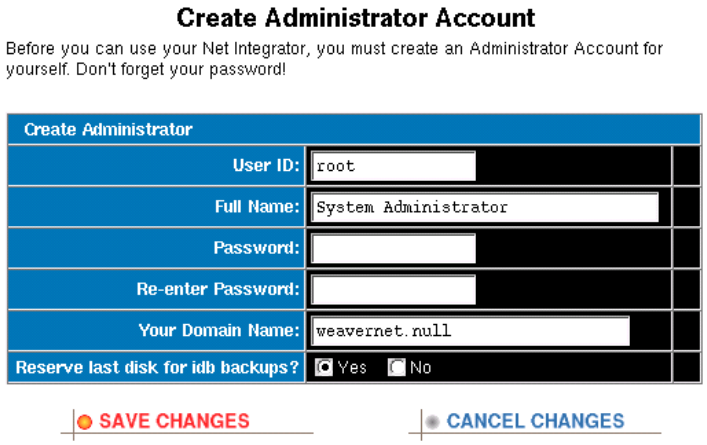
3. Select *Automatic* for location. Select *Built-in Ethernet* for connection. In the *TCP/IP* tab, select the *DHCP* configuration.
4. Click on the *Apply Now* button.
5. If the Internet connection doesn't function immediately, reboot your computer.

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:



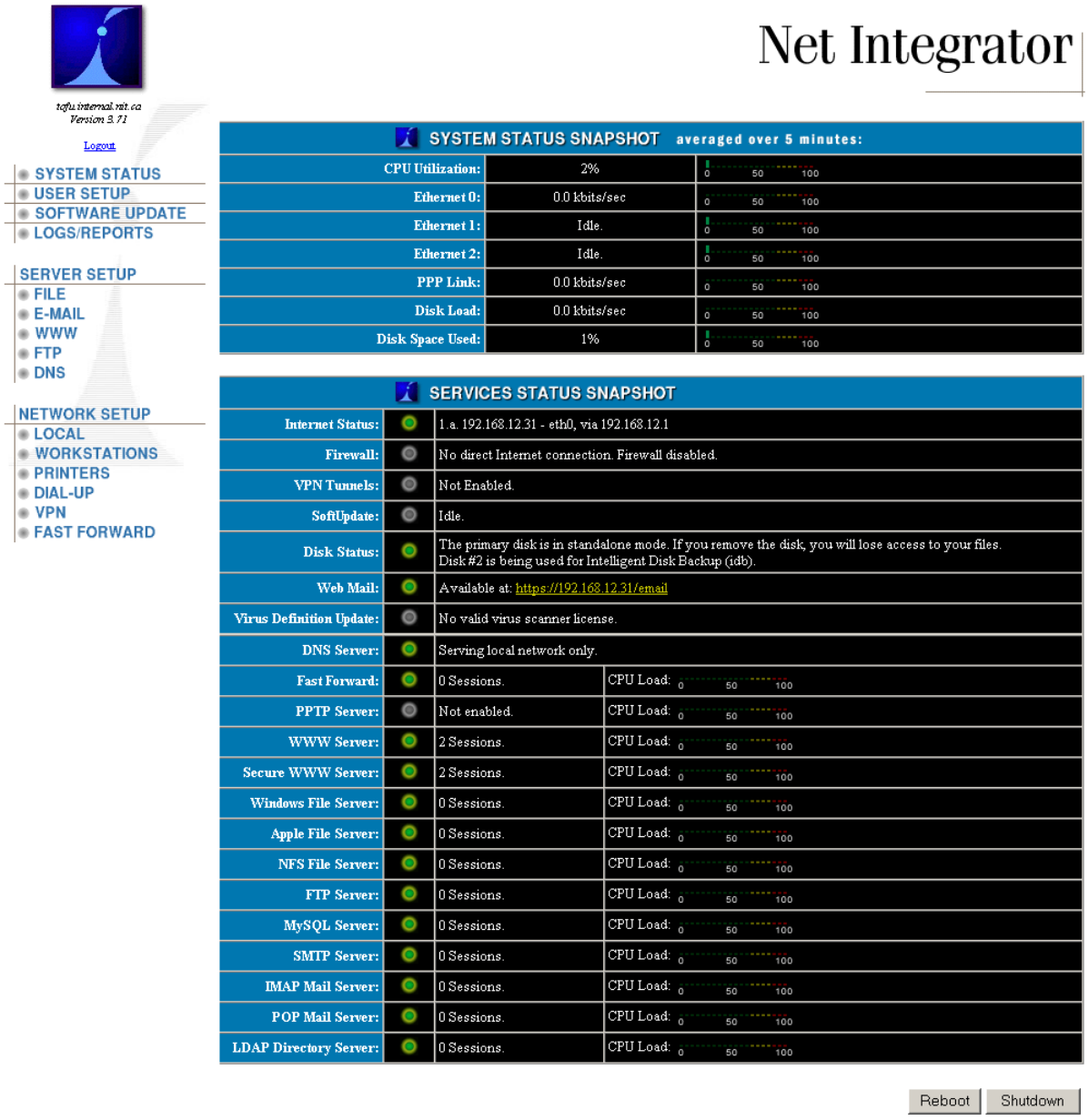
4. Enter a User ID. The default User ID is *root* – you can use that name or you can create a new ID by typing over the existing text.
5. Enter the administrator's full name.
6. Enter a password.
7. Re-enter your password to ensure it was entered correctly.
8. Enter your organization's registered Internet 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 22: 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 window 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.


Net Integrator
tofu.internal.nit.ca
Version 3.71
Logout
SYSTEM STATUS
USER SETUP
SOFTWARE UPDATE
LOGS/REPORTS
SERVER SETUP
FILE
E-MAIL
WWW
FTP
DNS
NETWORK SETUP
LOCAL
WORKSTATIONS
PRINTERS
DIAL-UP
VPN
FAST FORWARD
SYSTEM STATUS SNAPSHOT averaged over 5 minutes:
CPU Utilization: 2%
Ethernet 0: 0.0 kbits/sec
Ethernet 1: Idle.
Ethernet 2: Idle.
PPP Link: 0.0 kbits/sec
Disk Load: 0.0 kbits/sec
Disk Space Used: 1%
0 50 100
SERVICES STATUS SNAPSHOT
Internet Status: 1.a. 192.168.12.31 - eth0, via 192.168.12.1
Firewall: No direct Internet connection. Firewall disabled.
VPN Tunnels: Not Enabled.
SoftUpdate: Idle.
Disk Status: The primary disk is in standalone mode. If you remove the disk, you will lose access to your files. Disk #2 is being used for Intelligent Disk Backup (idb).
Web Mail: Available at: https://192.168.12.31/email
Virus Definition Update: No valid virus scanner license.
DNS Server: Serving local network only.
Fast Forward: 0 Sessions. CPU Load:
PPTP Server: Not enabled. CPU Load:
WWW Server: 2 Sessions. CPU Load:
Secure WWW Server: 2 Sessions. 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 rise above 100%. *This is normal.* One huundred per cent utilization simply means that the CPU is being fully utilized. Utilization above 100% (ie. 130%) means that if your CPU was 30% faster, it would be fully utilized at this point. Percentages above 100% do not mean that your Net Integrator is being overloaded or that performance will suffer, but if the CPU utilization exceeds 500%, service slow-downs may occur. You might want to upgrade your Net Integrator if this happens often.

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 56 kbps.

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, as a percentage.
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 *dial modem* 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).
VPN Tunnels	Displays the status of every active Virtual Private Network (VPN) tunnel (server-to-server/network-to-network).
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 grey. A red status light indicates a problem with the subsystem (usually an inability to access the distribution server). Refer to *Chapter 24: Log Messages* for more information on download errors.
Disk Status	Displays the status of your disk configuration, provides disk reconfiguration options, and displays the status of a rebuilding RAID array.
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 liscence, and the last reported updates.
DNS Server	Displays the status of the DNS server, and the last reported updates.

FastForward Displays the status of the port forwarding engine and the number of forwarded sessions. The status light is grey 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.

PPTP Server Displays the status of the PPTP server (which enables secure client-to-server VPN connections). The number of sessions shows how many users are connected. The status light is grey 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 grey 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 grey 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 grey 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 grey 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 grey 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 grey 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 NetIntegrator 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 grey 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 grey 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 grey 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 grey 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 *Shutdown* button means that your RAID array has to rebuild. See *Disk Status Messages* in *Chapter 22: Disk Management* for more information.

Chapter 3

Configuring your Net Integrator

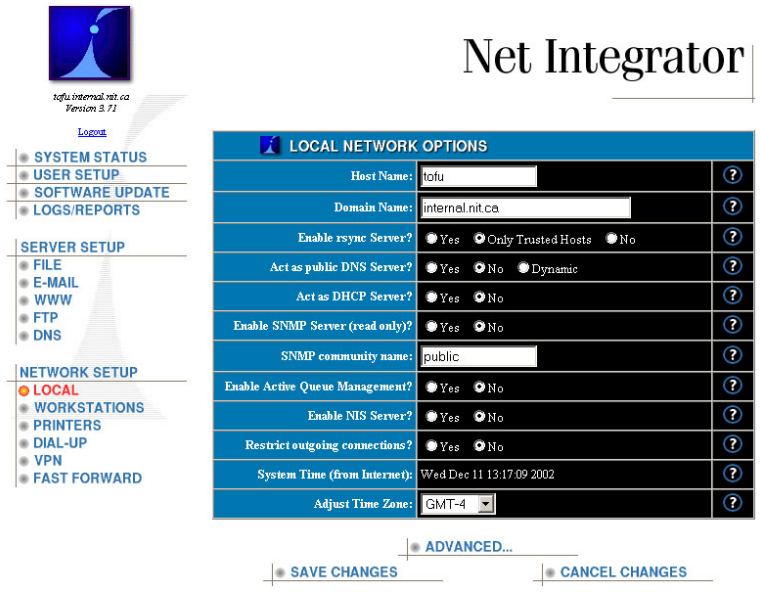
Proceeding with Configuration

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. Net Intelligence 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. Although the DHCP server is disabled by default, we recommend that you select *Yes* to enable it. Enabling the DHCP server means that IP addresses are automatically assigned to every workstation on the local network (as opposed to assigning them manually).

   Please Note: If there is more than one DHCP server on the local network, your Net Integrator will not activate its own DHCP server and will instead request automatic address assignment from the existing one. If Net Intelligence detects that DHCP requests are not being answered by any other DHCP servers, then the DHCP server is automatically enabled.

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 Net Integrator's ICSA certification, 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 18: 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.
13. Click on the *Save Changes* button.

Configuring Advanced Network Settings

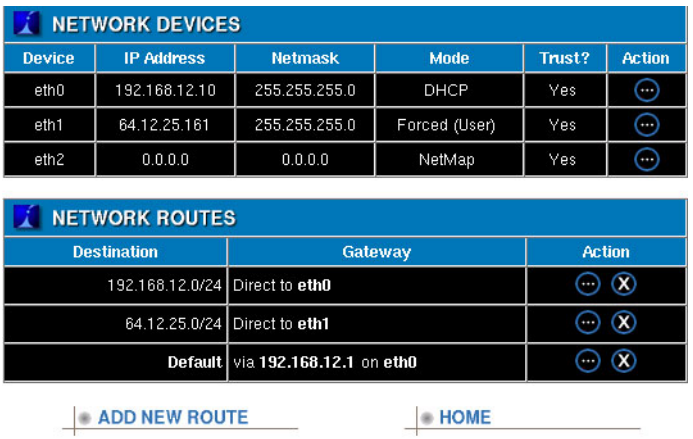
The *Advanced Network Settings* screen allows you to configure some of Net Integrator's more advanced features. Changing advanced network settings can cause odd behavior on your network; for example, if you change Net Integrator's IP address or Netmask to an incorrect value, you may not be able to reach 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 address. If Net Integrator boxes in various locations auto-configure their local network interfaces to the same network, 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

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

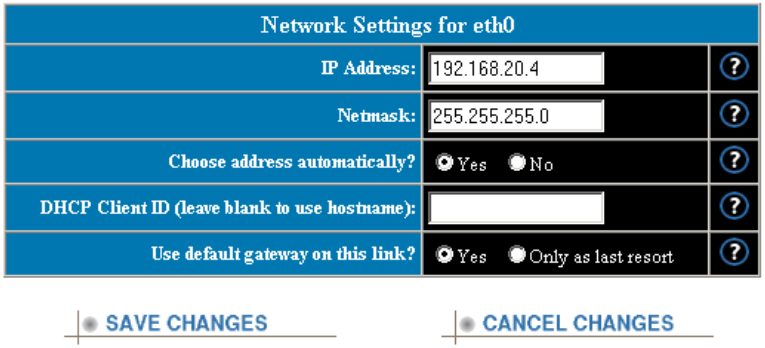
- **Device** – lists the network interfaces installed on Net Integrator. *Eth 0* should be connected to your LAN. *Eth 1*, *Eth 2,* and *PPP 0* should be connected to the Internet.
- **IP Address** – lists the IP addresses to the interfaces.
- **Netmask** – lists the IP network mask assigned to a particular 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:



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 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 addess 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).

6. **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.
7. **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.
8. 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).

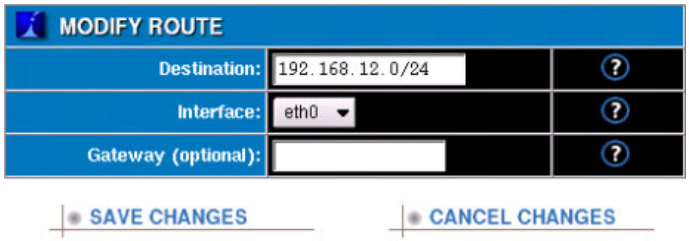
Please Note: Whether or not you have to change any route settings depends on your network setup and Net Integrator's connection to the LAN and to the Internet.

Deleting Network Routes

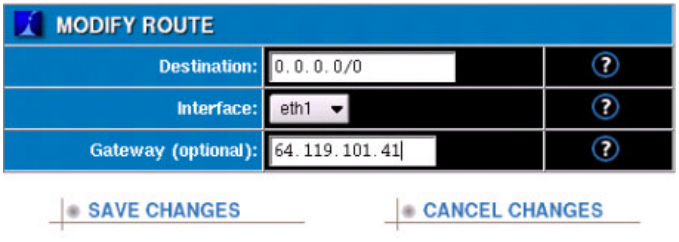
1. Click on the appropriate route's *Delete* button.
2. In the window that displays, click on the *Ok* button.

Editing Network Routes

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



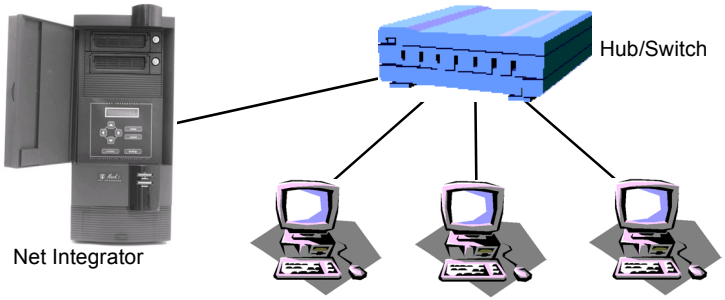
2. **Optional:** Enter a new destination IP address and netmask (in the format `192.168.12.0/24`).
3. **Optional:** Click on the *Interface* drop-down arrow and select the interface over which this network can be accessed.
4. **Optional:** If this is not a local network route entry (i.e. *eth1* or *eth2*),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



5. Click on the *Save Changes* button.

Network Configuration Scenarios

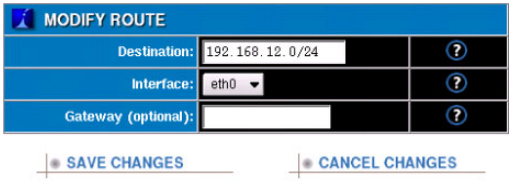
1. **Net Integrator as a Workgroup Server without a direct connection to the Internet**

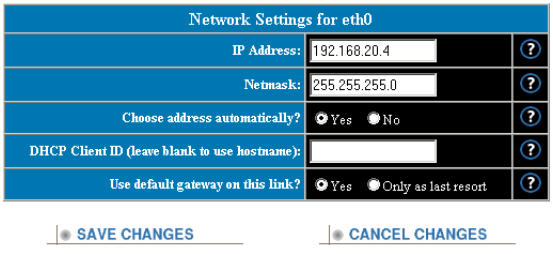


In this scenario, you would go to the *Advanced Network Settings* screen to change the IP address or the network mask of the local network interface or Net Integrator's default route. Although you generally do not need to change these settings, you can still do so:

f. In the *Network Devices* or *Network Routes* section of the *Advanced Network Settings* screen, click on the appropriate *Action* button.

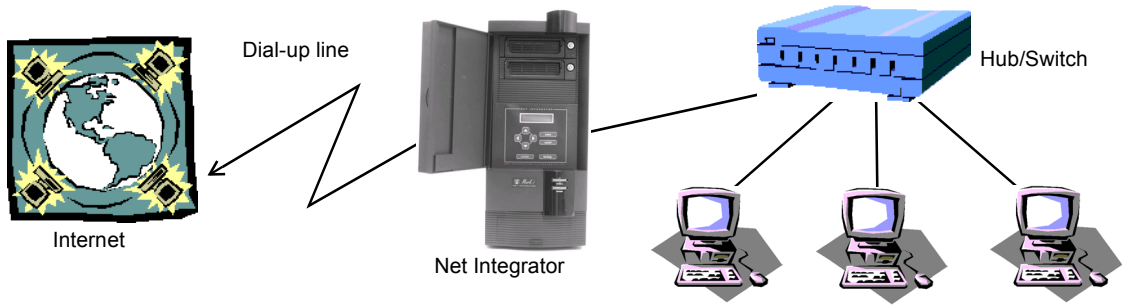
g. Depending on your choice, the *Modify Route* or the *Network Settings* screen displays:
Please Note: Refer to *Reconfiguring Network Devices* and *Reconfiguring Network Routes* earlier in this chapter for a full descriptions of these two screens.





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

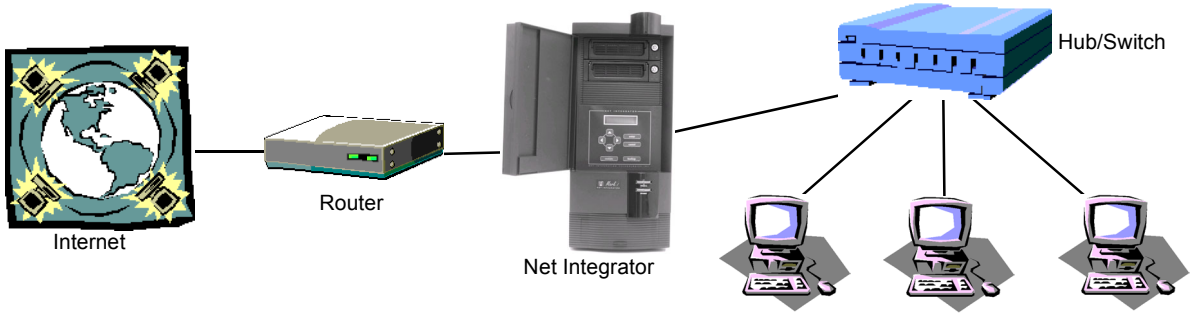
2. Net Integrator as a Workgroup Server and Dial-up Gateway to the Internet



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 autoconfigures 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:

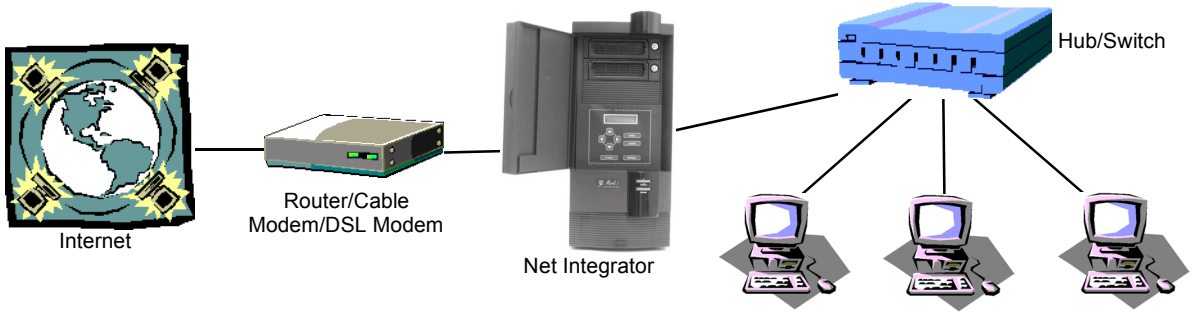
i. In the *Network Devices* section of the *Advanced Network Settings* screen, click on the *eth1 Action* button.

j. The *Network Settings* screen displays. Enter the new IP address and click on the *Save Changes* button.

k. In the *Network Routes* section of the *Advanced Network Settings* screen, click on the *Default Action* button (the last entry in the list).

l. 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

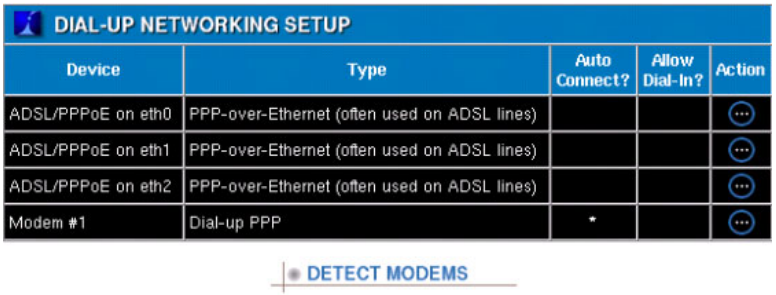


Net Integrator can serve as a Windows domain controller for all the compurters running Windows on the network. As the domain controller, Net Integrator will provide authentication services to the rest of the computers on the network. When this function is enabled, the Windows file server is set up as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

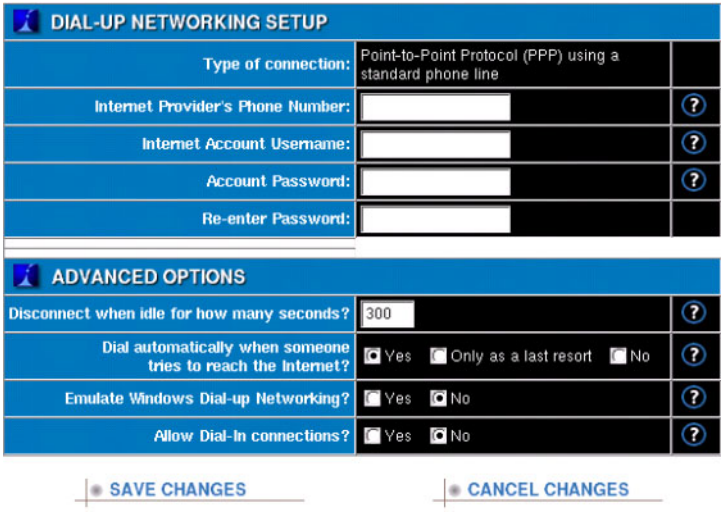
Configuring your Internet Connection

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:



2. **Optional:** If you have an external modem connected, you may need to do this to activate it: 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.
3. Click on the *Modem #1 Action* button. The following screen displays:

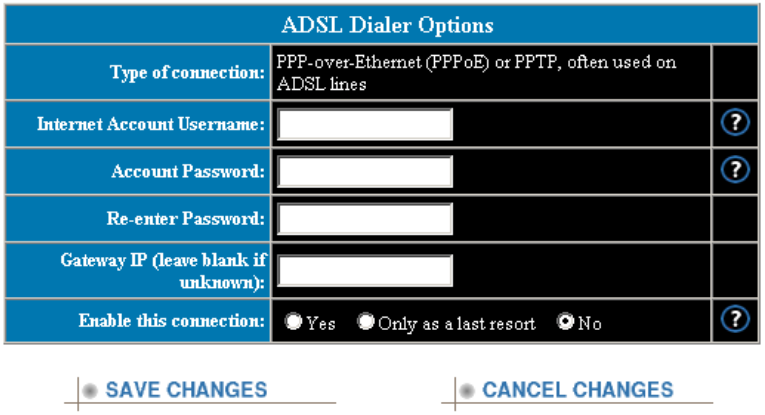


4. Enter the phone number provided by your ISP. If you have to dial 9 to get an outside line, enter this number as well. For example, enter: `9, 123-123-1234`.

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 do not have unlimited Internet access.
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)

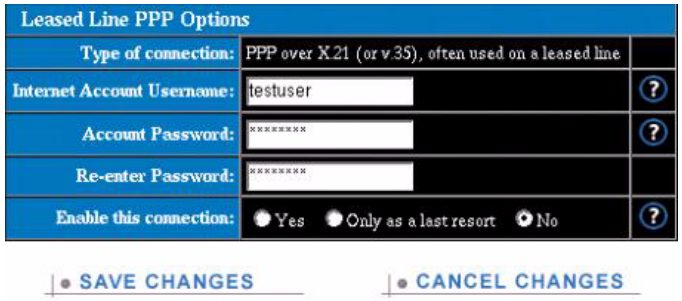
1. Select *Dial-up* from the *Network Status* menu found on the left side of any WebConfig screen. The *Dial-up Networking Setup* screen displays.
2. Click on the *Action* button in the appropriate ADSL row. The *ADSL Dialer Options* screen displays:



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:



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.

Chapter 4

DoubleVision

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 ISPs), 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**

Web browsers can share Internet links to improve browsing speed. For example, you could download an image using one Internet connection and download another image using another.

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 failover, 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

.

- **Dynamic DNS Integration**

If you're using Dynamic DNS, 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 19: Domain Name Services* for more information.

- **Net Intelligence**

No human intervention is required to activate and deactivate Internet services when they fail or are restored. Net Intelligence 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.

You can take advantage of DoubleVision even if you do not have access to a high-speed Internet connection. Simply configure more than one modem by indicating that you want both of them to dial automatically when someone tries to reach the Internet. In addition, you can configure one or more modems as a 'last resort' option (in case the primary modems fail). For more information on configuring a modem, refer to *Chapter 3: Configuring your Net Integrator*.

Please Note: 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.

Chapter 5

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 or IMAP mailboxes.

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`

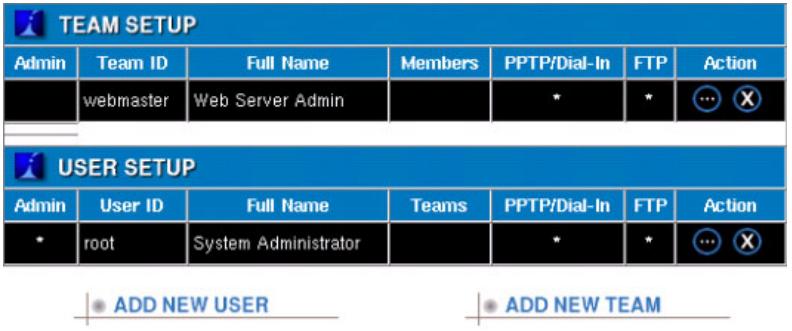
to access this directory. For example, the path for a team named *sales* would be `/export/home/sales`.

- 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 are automatically forwarded to all members of the team.

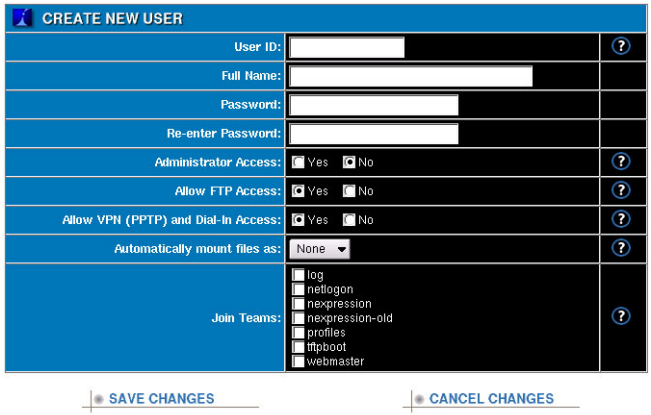
User Accounts

Creating Users

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



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



3. 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, jane_doe*).

   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`.

4. Enter the user's full name.
5. Enter a password for the user. User passwords should be unique.
6. 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.
7. 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.
8. 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.

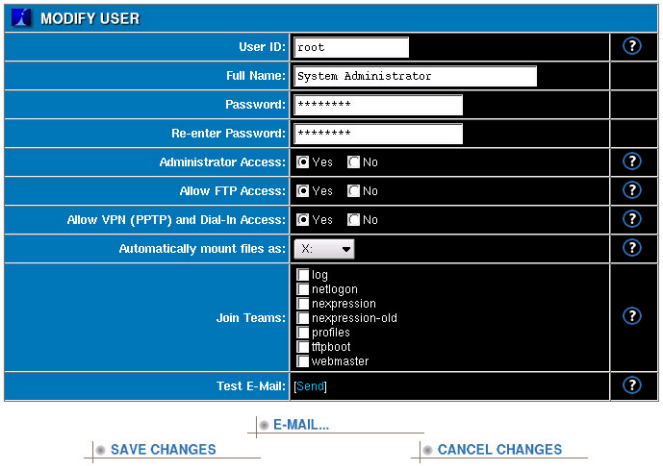
9. Indicate whether or not the user is allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most users should not be able to establish a remote connection.

   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 17: 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 redisplays, 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:



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 *Send* to send this user a test email.
4. Click on the *Saves Changes* button.

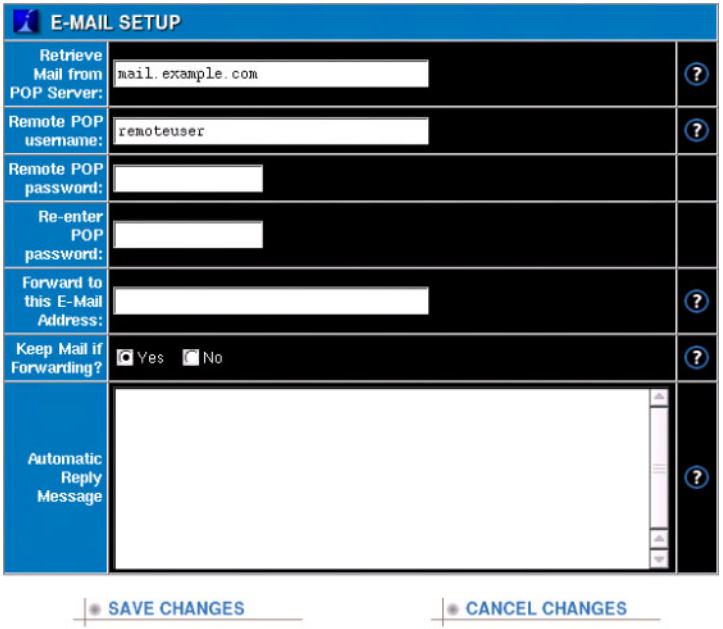
Deleting Users

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. In the window that displays, click on the *OK* button.

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



4. **Optional:**

   m. In the *Retrieve Mail from POP Server* field, enter the server on which the user's POP account it is located.

   n. Enter the user's remote POP password. This field has to be filled in the following format: `username@mailserver`. For example, if the user's POP username is *johndoe* and his email is stored in the `mail.example.com` or `192.168.0.1` server, you would enter `johndoe@mail.example.com` or `johndoe@192.168.0.1`.

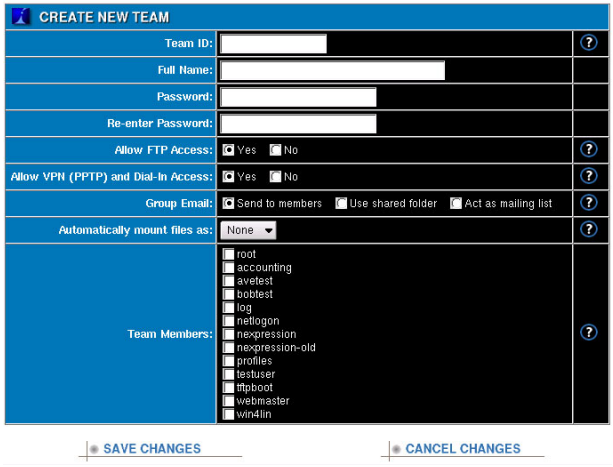
   Please Note: Enter information into these fields only if Net Integrator is not your primary mail server or if you have another mail account that you want to have retrieved along with your Net Integrator mail. This should only be used if you are retrieving mail from an alternative, secondary source (ie. above and beyond Net Integrator's mail services)

5. Enter a remote POP password.
6. Re-enter the 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.
7. **Optional:** Enter an email address to which the user's emails should be forwarded.
8. Indicate whether or not you want emails to be kept on the server after they have been forwarded. This is typically done if a user has emails forwarded to them while they are on vacation or out of the office.
9. **Optional:** Enter a text message to be sent automatically to any received emails. This is typically done to inform people that the user will be out of the office or to notify the sender that their message was received.
10. Click on the *Save Changes* button.

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



3. 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*).
4. Enter a descriptive name for the team in the *Full Name* field.
5. Enter a login password for the team. Team passwords should be unique.
6. 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.
7. 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.

8. 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 17: Remote Access Services* for more information.

9. 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.

     The backend for the mailing list is a program called ezmlm. For example, mail sent to group@example.com is handled by .qmail and is forwarded out to all subscribed people by ezmlm.

     Mail sent to group-owner@example.com is fastforwarded to all members of the team (the members act as administrators on a mailing list team) by .qmail-owner. Mail sent to group-(anything else)@example.com is handled by .qmail-default.

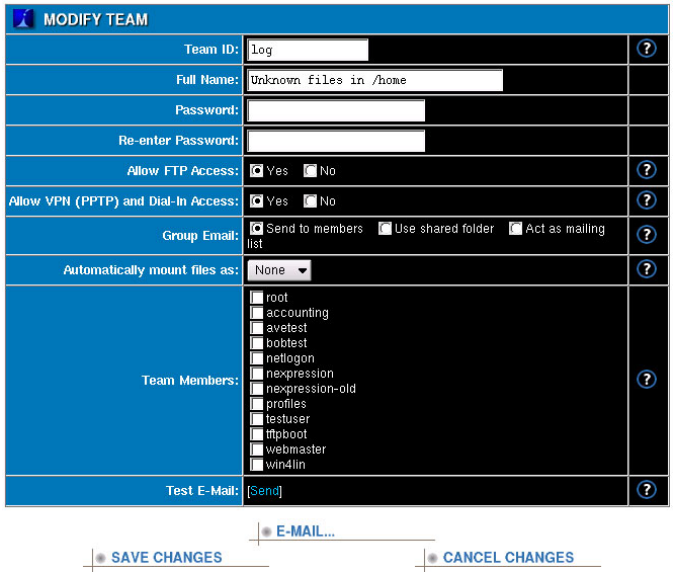
     When a mailing list is first set up, no one is subscribed to it. People who want to subscribe (including group members) must do it themselves. To subscribe/unsubscribe, mail is sent to group-subscribe@example.com or group-unsubscribe@example.com.

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

     The default value for a group email is to forward mail to all members. See WvAuth::sync_user() for specifics on how this is set up and maintained.
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 redisplays. 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 the *Save Changes* button.

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.

Chapter 6

File Services

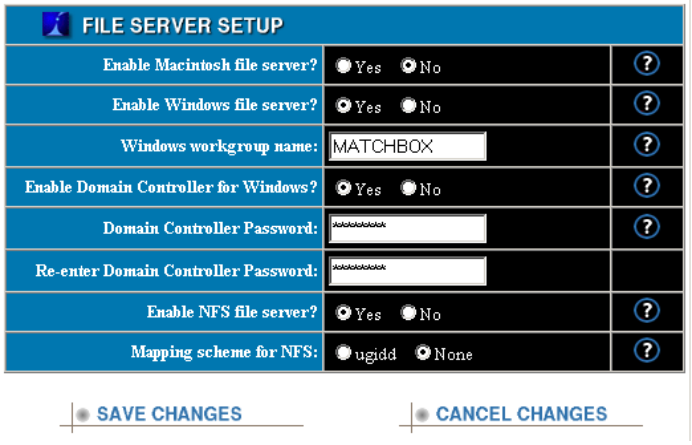
File Sharing Services

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:



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 is the 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.

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*.

Chapter 7

Domain Controller

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.

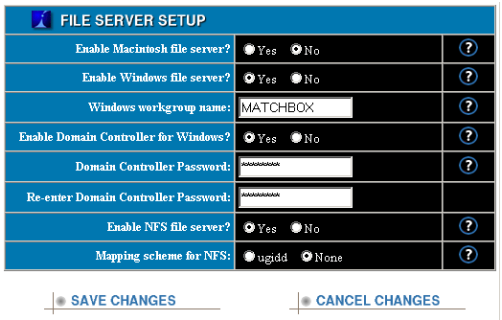
Net Integrator can serve as a Windows domain controller for all the computers running Windows on the network. When this function is enabled, the Windows file server is set up as a domain controller, and a domain will replace the Windows workgroup.

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

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:



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.

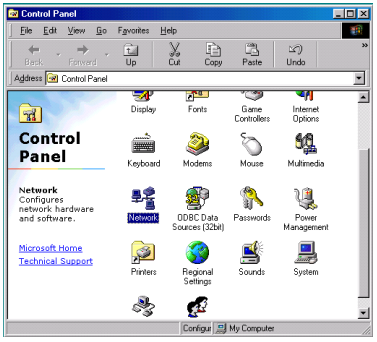
Joining Windows Systems to a Domain

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*.

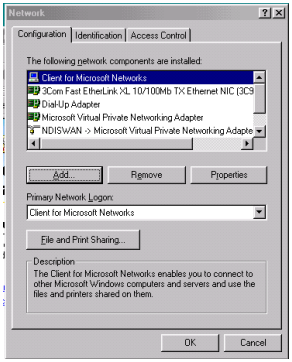
For Windows 95/98/ME:

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:

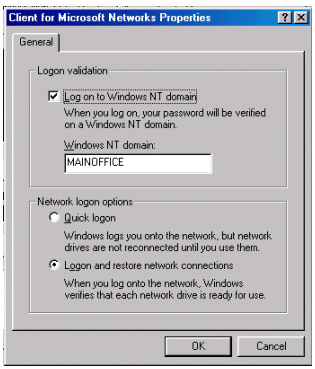
1. In Windows, select *Start* > *Settings* > *Control Panel*. The *Control Panel* window displays:



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



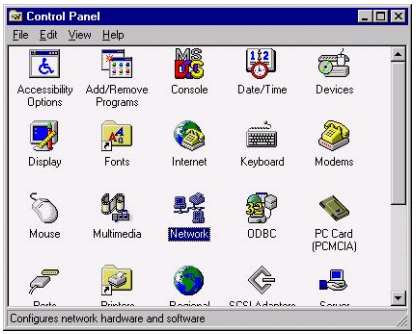
3. From *The following network components are installed* list, select *Client for Microsoft Networks*. Click on the *Properties* button. The *Client for Microsoft Networks Properties* window displays:



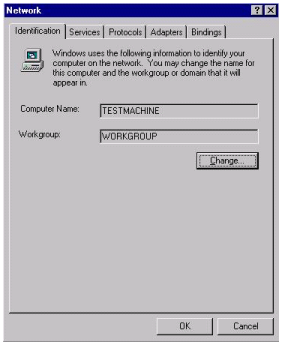
4. Check the box for *Log onto Windows NT domain* and enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Click on the *OK* button. The *Network* window displays. Click on the *OK* button again.
6. Reboot the workstation. The next time you log on, the login window will have an additional *Domain* field.

For Windows NT:

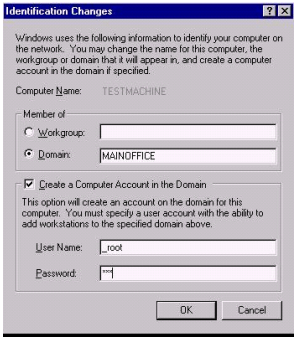
1. In Windows, select *Start* > *Settings* > *Control Panel*. The *Control Panel* displays:



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



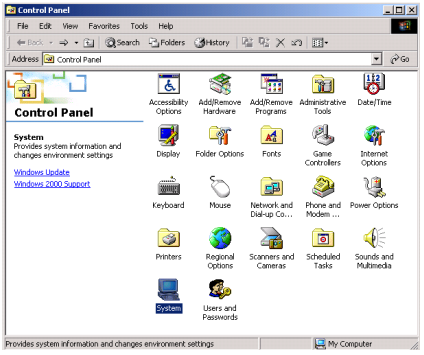
3. Click on the *Change* button. The *Identification Changes* window displays:



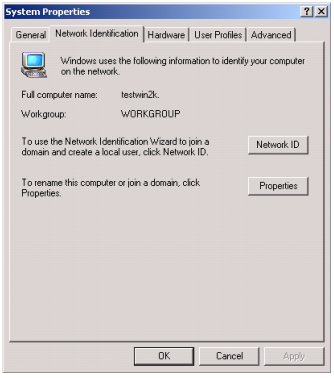
4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Check the box for *Create a Computer Account in the Domain*. Enter the administrative username, *_root*, and the 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:

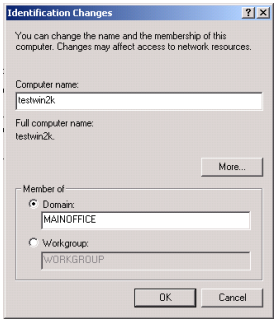
1. In Windows, select *Start* > *Settings* > *Control Panel*. The *Control Panel* displays:



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



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

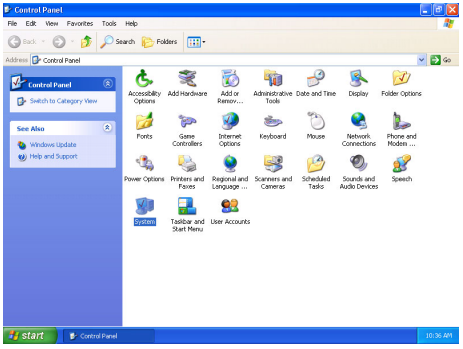


4. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
5. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

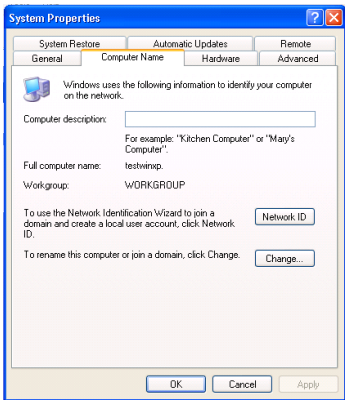
For Windows XP:

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

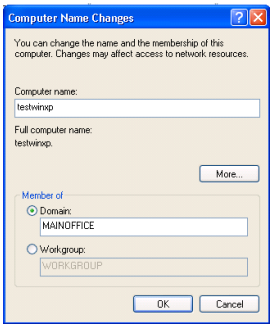
   For information on the latest features available in Samba as a domain controller, download this PDF: http://www.net-itech.com/america/support/docs/csamba6.pdf
2. In Windows, select *Start* > *Control Panel*. The *Control Panel* window displays. On the left menu bar under *Control Panel*, select *Classic 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:



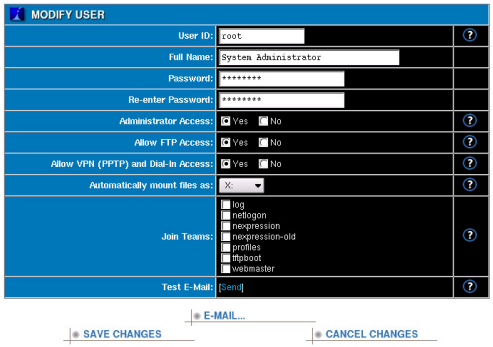
5. In the *Member of* section of the window, select *Domain*. Enter the name of the domain (as entered in the *Windows workgroup name* field on the *File Server Setup* WebConfig screen).
6. Click on the *OK* button. The next time you log on, the login window will have an additional *Domain* field.

File Mounting

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:



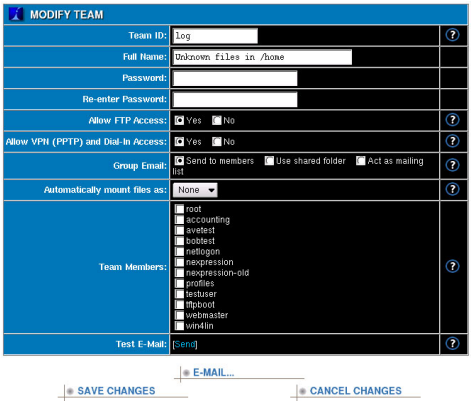
2. From the drop-down menu in the *Automatically mount files as* field, select the drive that the user's files should be mounted as on the workstation. The default drive is *X:*.
   Please Note: Be sure to choose a drive that will not conflict with drives already in use.

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:



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.

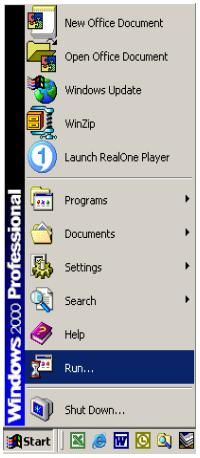
This can also be done when the team is created.

Import Users from Windows

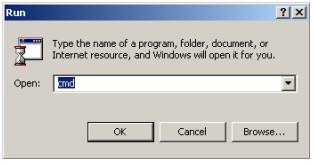
To upload user information from a Windows 2000 or NT server:

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.

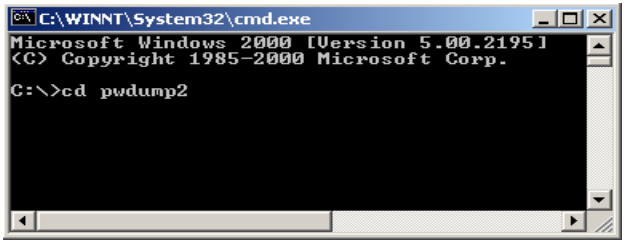
3. Click on the *Start* menu, and choose *Run*.



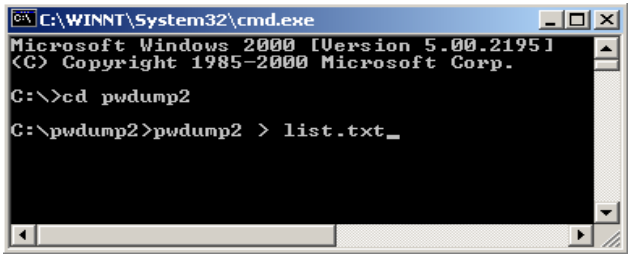
4. Enter "cmd" and click *OK*.



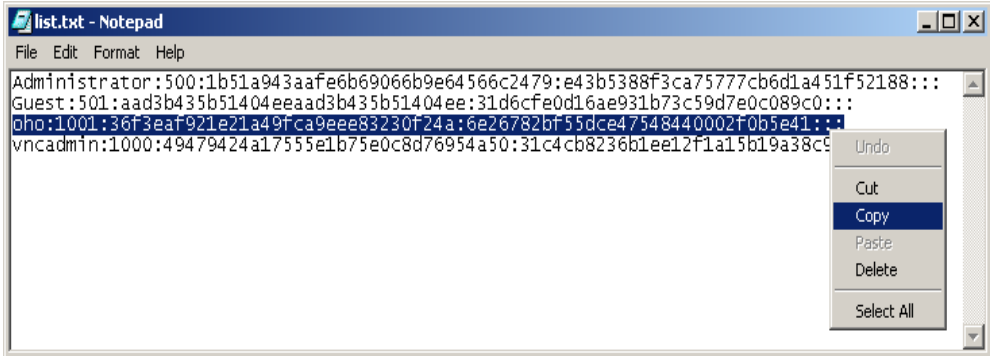
5. Type "cd pwdump2" and hit *Enter*. This will change the directory to the folder you created on your C drive that contains the contents to the file "pwdump2.zip".



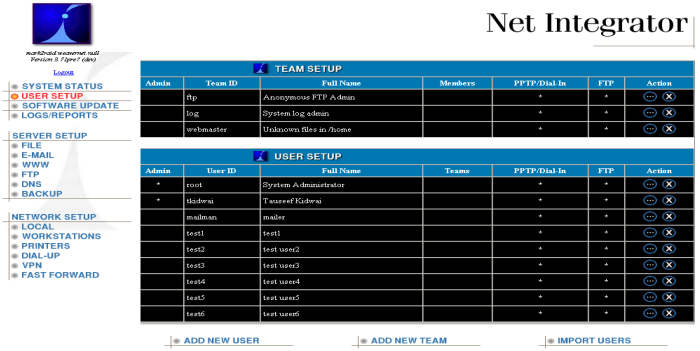
6. Type “pwdump2 > list.txt” and hit Enter. This will run the file called “pwdump2.exe” and generate a text file called “list.txt” in the same folder.



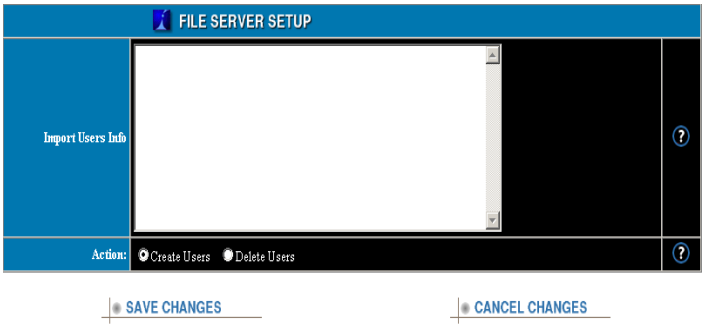
7. Open the file called “list.txt”. This contains a list of Windows users. Highlight the users you wish to import, right-click with your mouse and choose *Copy*.



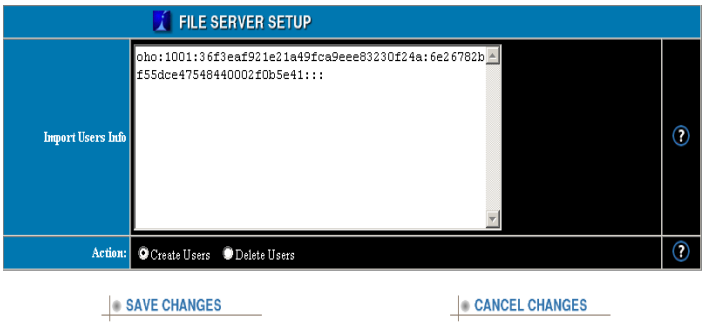
8. In WebConfig, click on *User Setup* in the left-side menu.



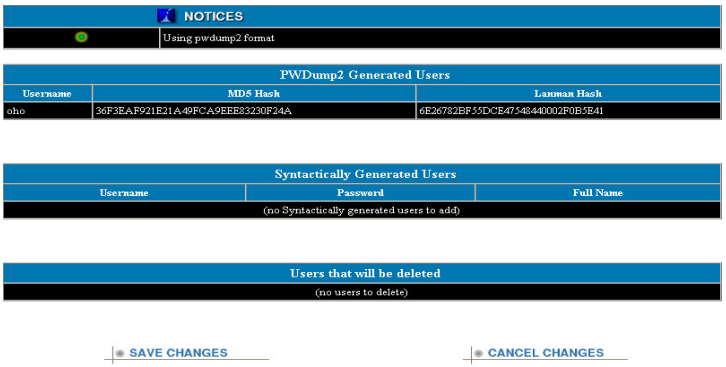
9. Click on *Import Users*. This screen will display.



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.

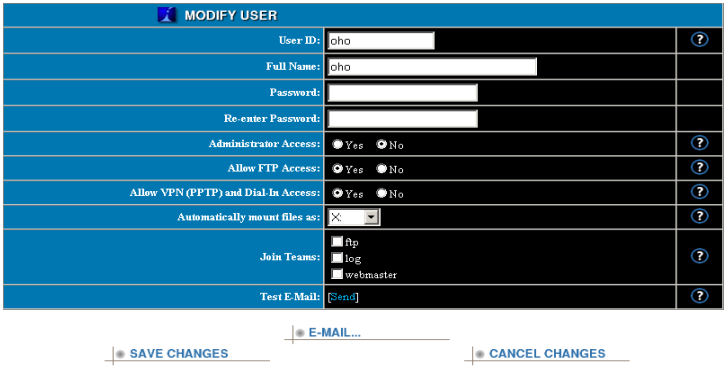


11. Click on *Save Changes*. This screen will display.



12. Click on *Save Changes*.

13. For each of the imported users, an Administrator will have to create passwords. To do this, click on the left button in the *Action* column, in the row containing a user's information. This screen will display.



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

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.

Chapter 8

Print Services

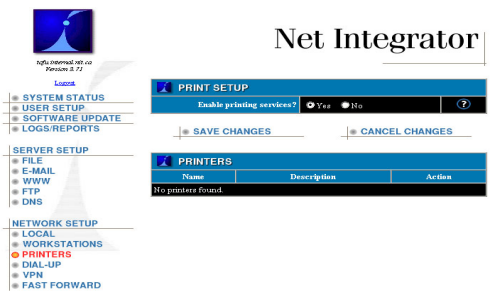
Net Integrator Print Services

Net Integrator's parallel printer port can be connected to any type of printer that users are sharing on the internal network. You can also use ethernet printer sharing devices to connect printers directly to your LAN. 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).

Configuring Print Services

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

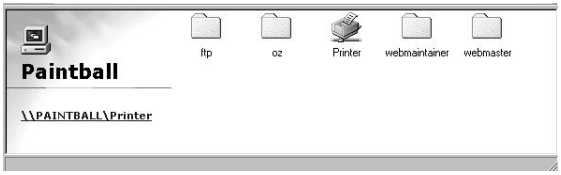
1. Click on the *Printers* button on the WebConfig screen. Net Integrator will list all the available printers.



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.

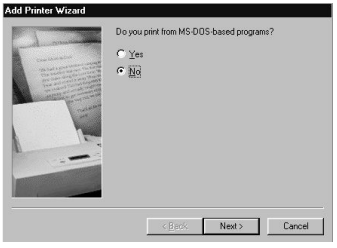
Configuring your Workstation

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:

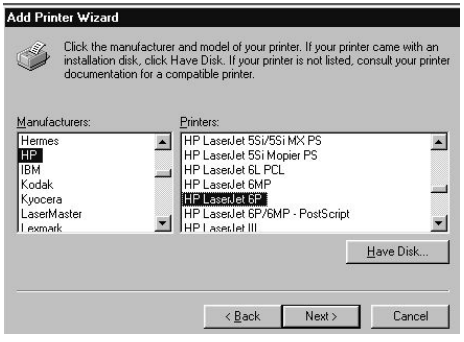


2. Double click on the printer icon. The following window displays:

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

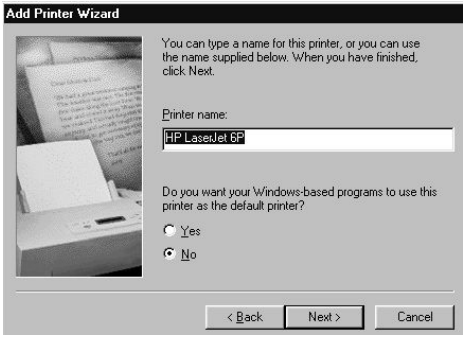


4. Select *No* to indicate that you are not printing from MS-DOS programs. Click on *Next*.
5. Select the brand and type of printer that is connected to your Net Integrator. Click *Next*.

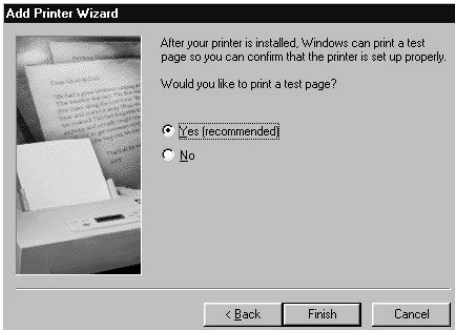


Please Note: If your printer is not listed, click on the *Have Disk* button and provide the printer driver from the disk provided by your printer's manufacturer.

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.

Chapter 9

Email Services

Components of the Email System

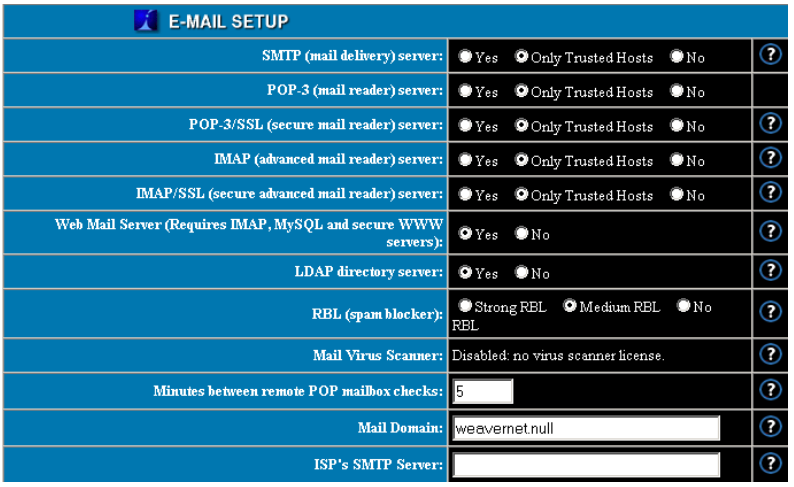
The main components of Net Integrator's email delivery subsystem are the:

- **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.

- **Realtime Blackhole List (RBL) –** a 'spam' blocker that has different levels of spam protection (such as *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:



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 E-Mail 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.

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:

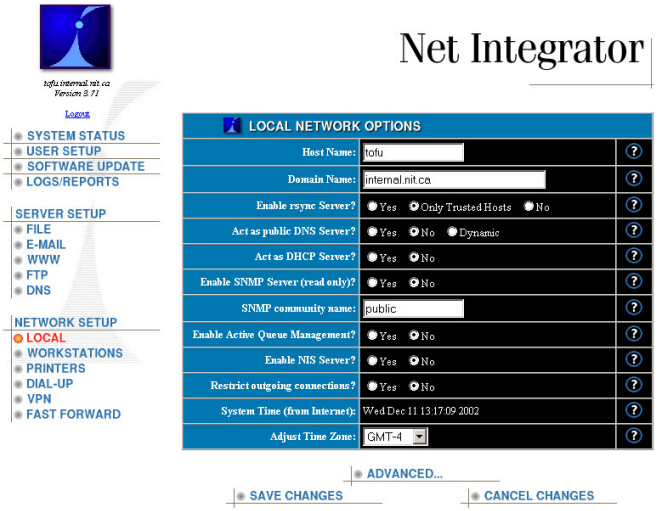
MX records for your domain should be pointed to your Net Integrator's outside IP address (the address assigned to the eth1 interface).

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:



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.

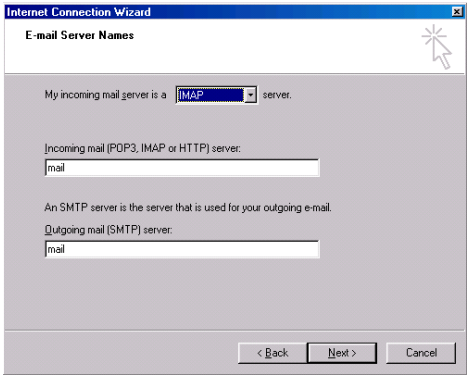
1. **If your mail is hosted on your ISP's mail server...**
   All users in your office have their own mail address and mailbox hosted on the ISP's server. Your ISP supplies you with the name of the POP3 or IMAP server where your mail has to be retrieved and with the address for the SMTP mail delivery 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:

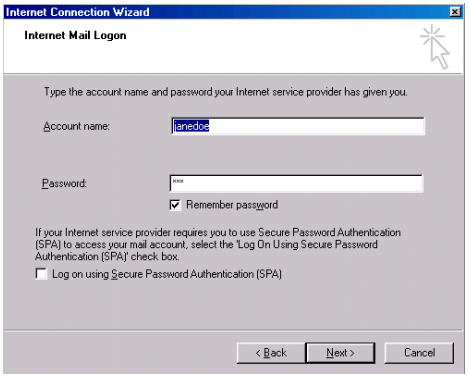
- In the *SMTP server* field, enter the IP address or host name provided to you by your ISP. Alternatively, use your Net Integrator as the SMTP server and enter the IP address or host name of your Net Integrator.
- In the *POP3* or *IMAP server* field, enter the IP address or host name provided to you 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 retreive 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.

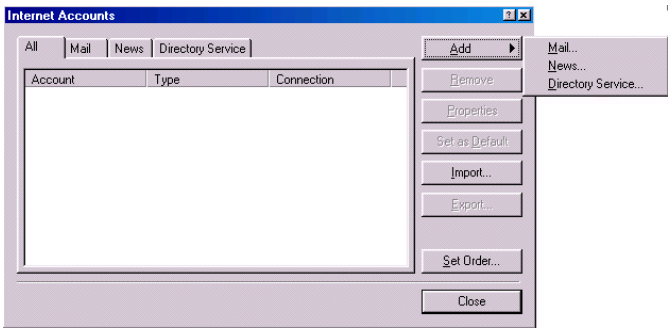
Please Note: To modify user's advanced email settings, refer to *Modifying User Email Settings* in *Chapter 5: User & Team Management.*

LDAP Server

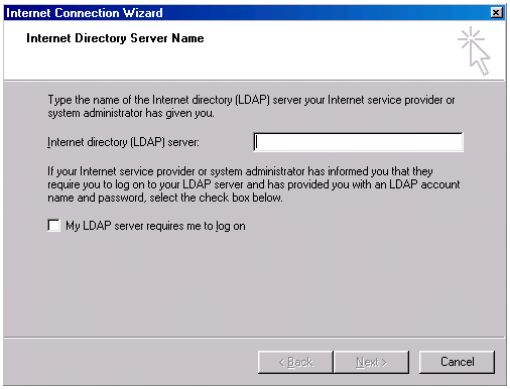
Net Integrator has a built-in Lightweight Directory Access Protocol (LDAP) server, which provides a directory of user names and email addresses. It is automatically populated with names and email addresses of all Net Integrator users. Most email clients support access to read-only LDAP servers.

Configuring LDAP in Microsoft Outlook

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

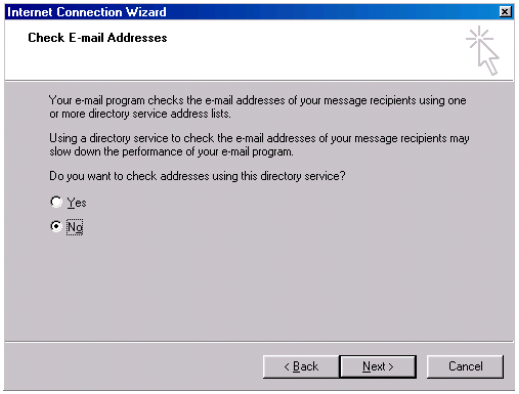


2. Select *Add* > *Directory Service*. The *Internet Connection Wizard* displays:



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

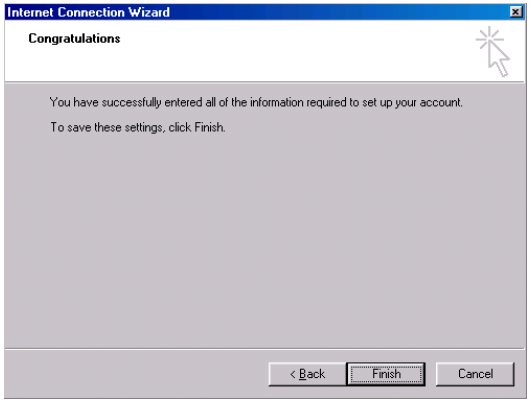
4. Click on the *Next* button. The following screen displays:



5. Indicate whether or not you want your email client to check addresses using the LDAP directory.

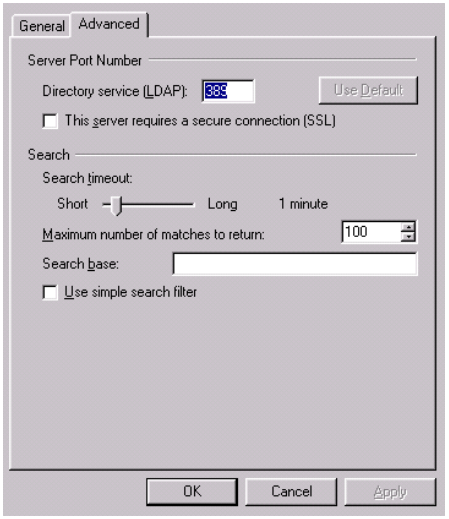
   Please Note: If this option is selected, you can enter partial email addresses when sending emails. Outlook will automatically find the closest match in the LDAP directory and enter the correct email address.

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



7. Click on the *Finish* button. The *Internet Accounts* screen redisplays. 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 redisplays. 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.

Chapter 10

WebMail

WebMail Server

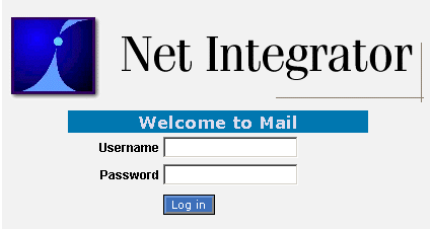
Net Integrator's WebMail server allows you to access your email using a standard web browser from any workstation connected to the Internet. Your communications are kept secure with SSL encryption.

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/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 `192.138.0.1`, enter `http://192.168.0.1/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:

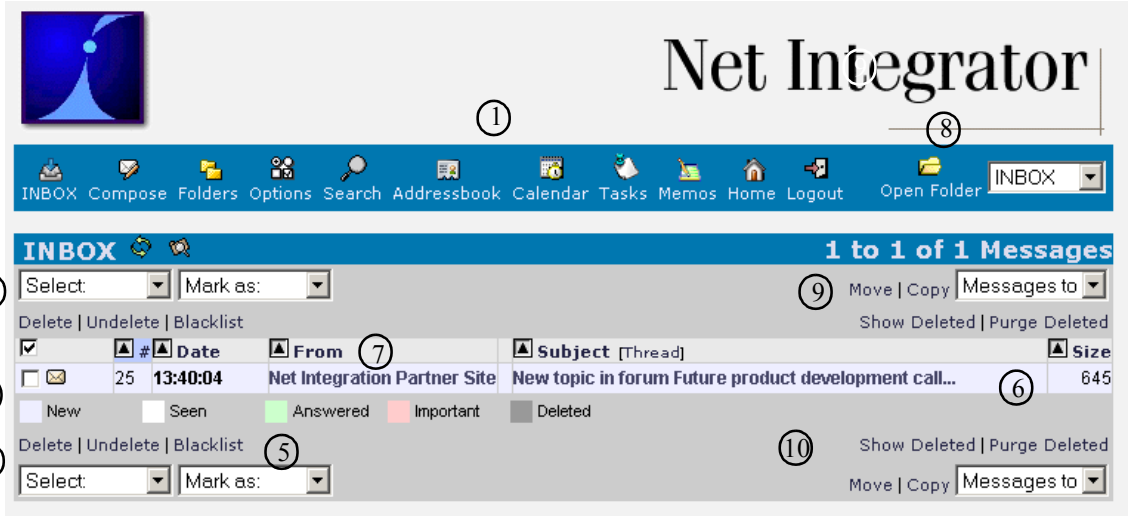
Please Note: This alerts the user that the security certificate presented by Net Integrator cannot be verified for authenticity. If you want a certificate that is authenticated by a certificate authority, you will have to purchase one. Please refer to *Chapter 11: Web Services* for more information.

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



5. 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



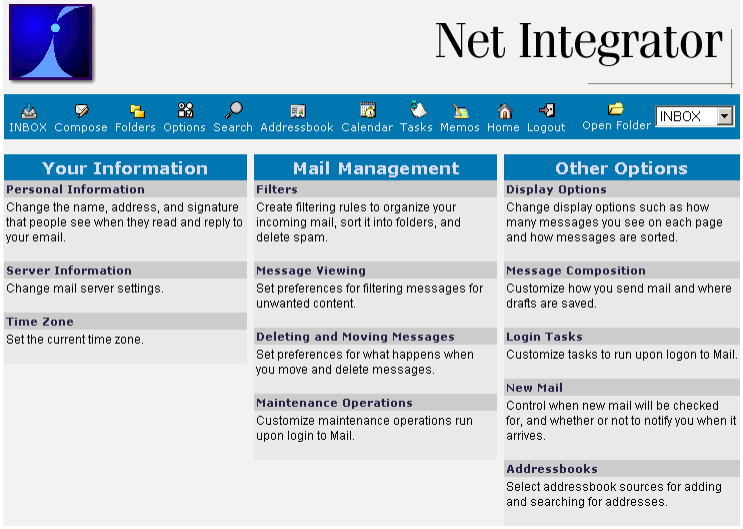
1. From the *Main Webmail Menu,* click on the:
   - *Inbox* button to view the contents of your inbox.
   - *Compose* button to compose a new email message. See *Composing an Email Message* for more information.
   - *Folders* button to view a screen that lists your folders. On this screen, you can create, 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

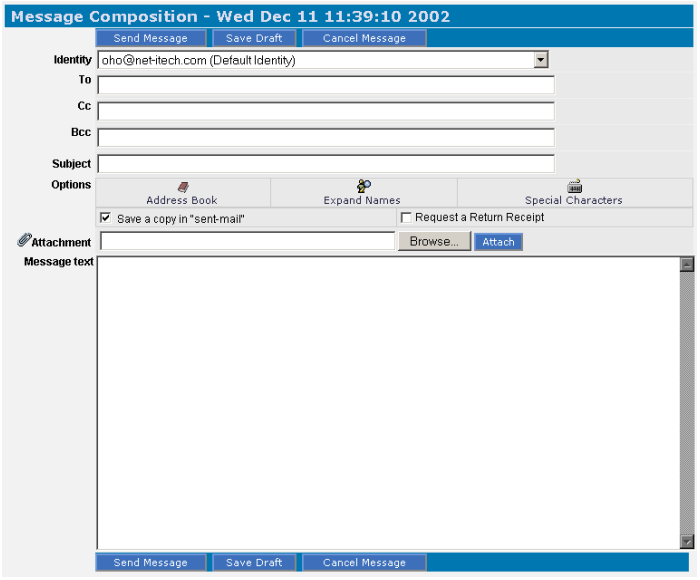
1. From the *Main WebMail Menu,* click on the *Options* button. The *Options* screen displays:



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 `johndoe@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.

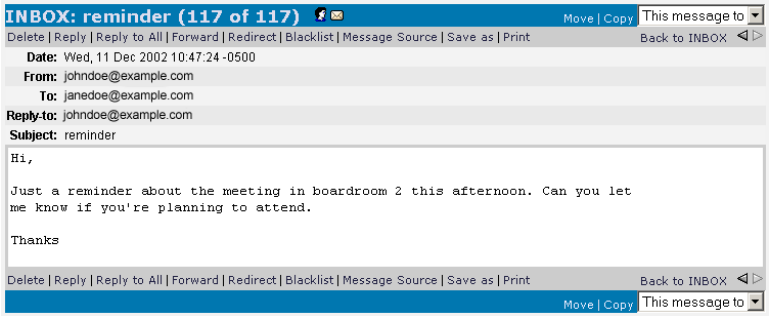
    Please Note: To remove an attachment, place a check in the attachment's checkbox and click on *Remove Selected*.

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 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.

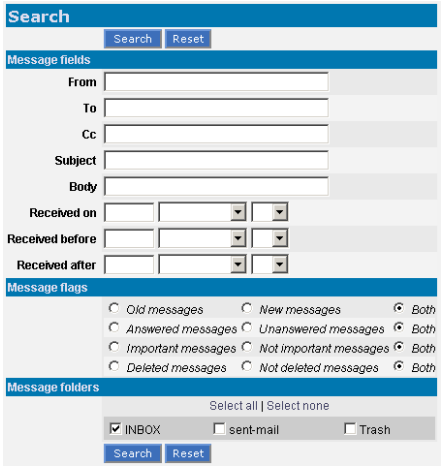
Replying to a Message

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 correspondance 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* funtion 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:

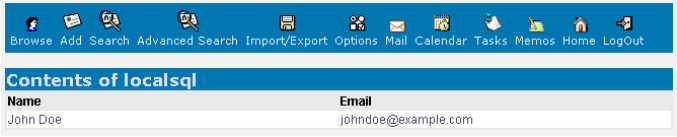


2. Enter information into the appropriate *Message fields*.
3. Select the appropriate *Message flags*.
4. Select the appropriate *Message folders.*
5. Click on the *Search* button to begin the search.
   Please Note: Click on the *Reset* button prior to clicking on the *Search* button to clear your search 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:



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.

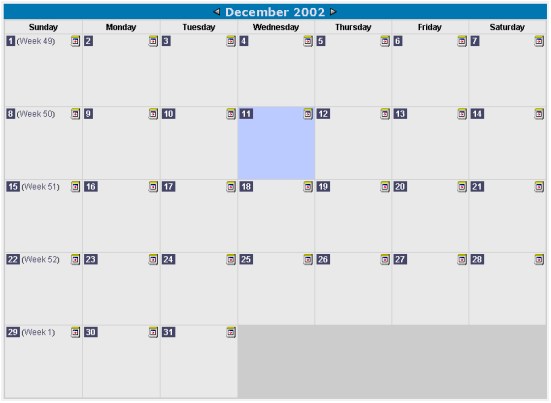
Importing and Exporting Addresses

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.

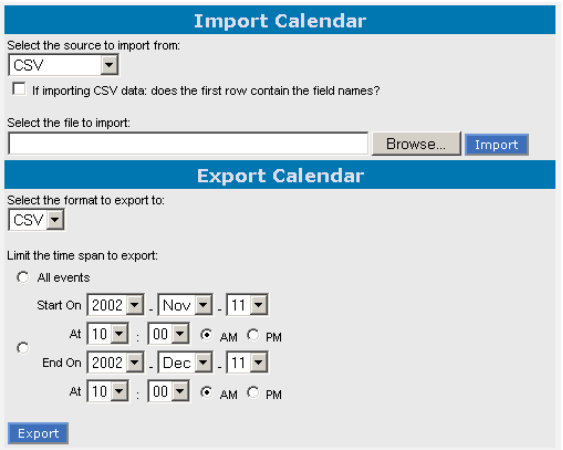
Calendar

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:

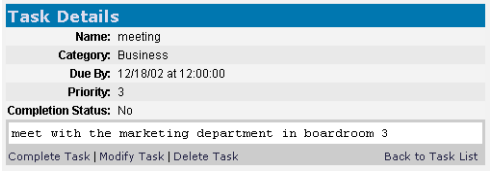


- In the *Import Calendar* section of the screen, select the format to export from (your options are *CSV* and *Outlook*).
- Select the file to import. Either enter the file name directly into the empty field or select it by clicking in the *Browse...* button.
- Click on the *Import* button.

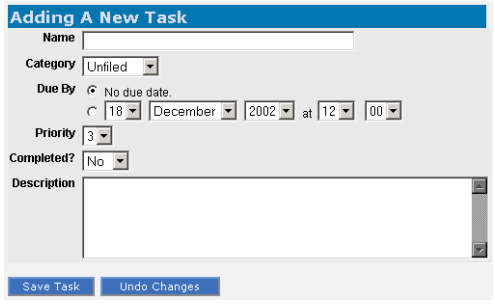
6. To export a calendar to another source:
   - Click on the *Import/Export* button. The *Import/Export* screen displays.
   - In the *Export Calendar* section of the screen, select the format to export to.
   - Select the exporting time span.
   - Click on the *Export* button.

Tasks

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



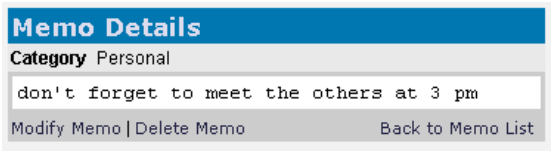
2. To add a new task, click on the *New Task* button. The following screen displays:



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:



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

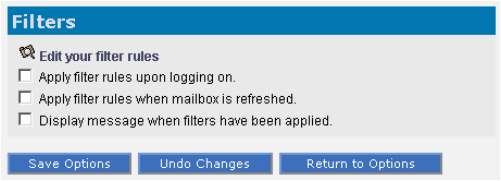
3. Enter the appropriate text.
4. Click on the *Save Memo* button. Your list of memos will appear.
5. To delete your memos, click on the *List Memos* button. Place a check next to any memo that you want to delete, then select *Delete Memos* from the pull-down menu.

Mail Filters

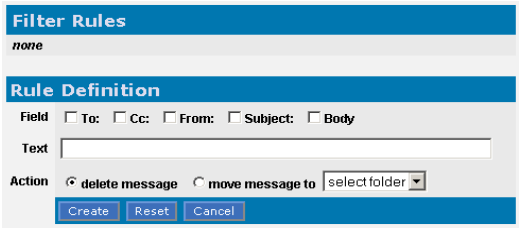
By applying rules based on message headers or content, mail filters allow you to automatically move messages to certain folders or delete messages from your inbox.

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:

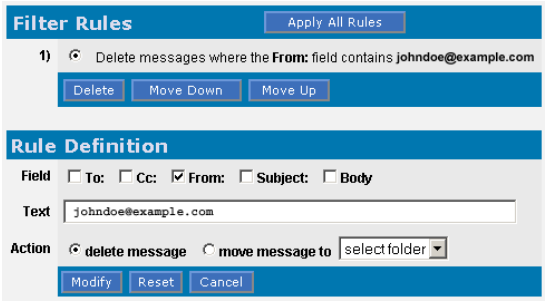


3. Select the appropriate field.
4. Enter the appropriate text.
5. Select an action. Place a check in the *delete message* box if you want mail that fits the rule to be deleted. Place a check in the *move message* box and select a folder if you want mail that fits the rule to be moved to a specific folder.
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 redisplays.

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 delete and click on the *Move Down* or *Move Up* button.

Chapter 11

Web Services

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 a *Virtual Web Server*.

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.

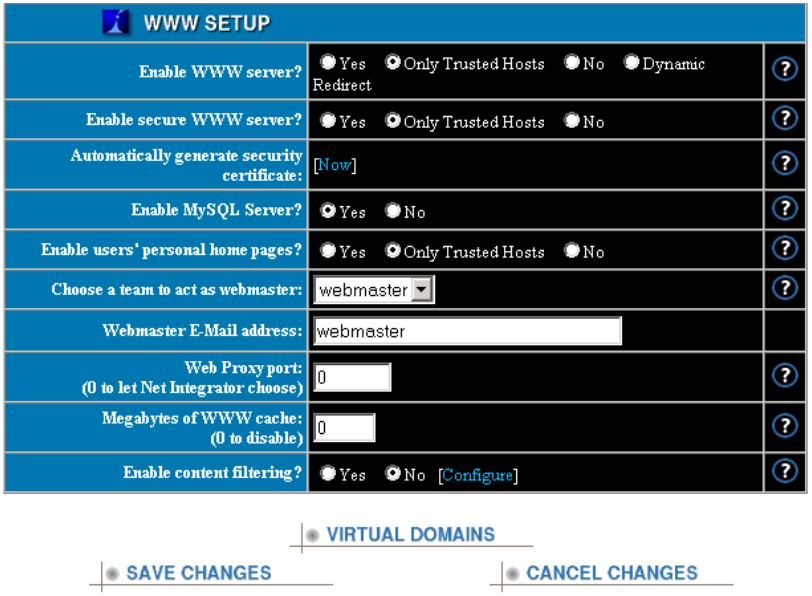
Webmaster Directory

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:



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 19: 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. **Optional:** Click on the *[Now]* button to generate a security certificate. Although a certificate is automatically generated the first time you power-up Net Integrator, you can generate a new certificate to overwrite the old one at any time.

   IMPORTANT:DO NOT generate a new certificate if you have purchased a security certificate from a certificate authority and placed in the Webmaster directory. Doing so overwrites the purchased certificate with the one generated by your Net Integrator. To protect your purchased security certificate, you may want store a copy of it in a different directory.

5. 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 23: 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 forWebMail 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.

6. 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*.
7. 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.
8. Enter the email address of the *Webmaster* (the person who is in charge of this web site).
9. Enter the appropriate number in the *Megabytes of WWW cache* field. Refer to *Web Caching* (in this chapter) for more details.
10. Click on the *Save Changes* button.

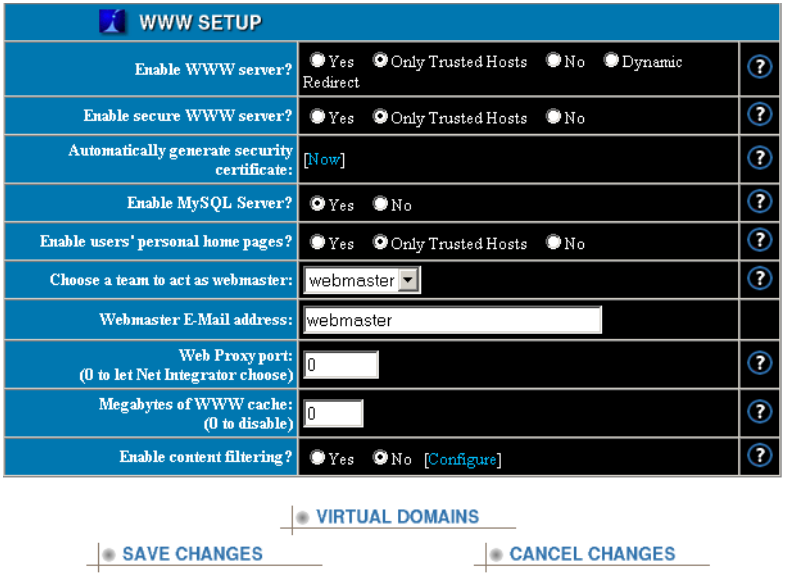
Virtual Web Servers

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).

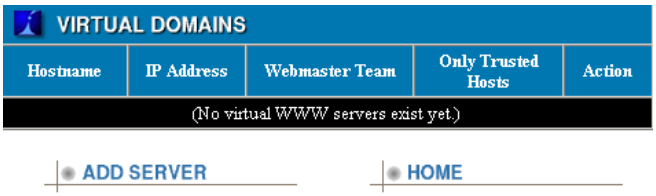
Every virtual web site has to be associated with a maintenance team (which can maintain only one virtual web site). This means that for every virtual web site that you create, you also have to create a team that will maintain it. If this site is maintained by users on the local network, they can be made 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

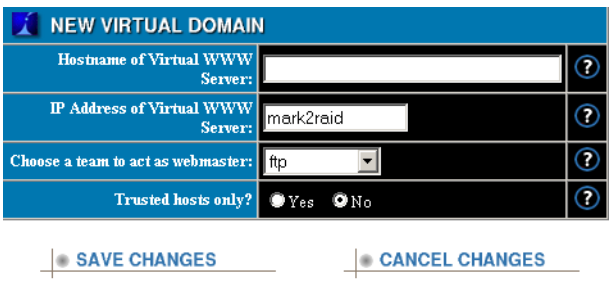
1. Select *WWW* from the *Server Setup* menu on the left side of any WebConfig screen. The *WWW Setup* screen displays:



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



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



4. 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.
5. 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.
6. Select a team to perform Webmaster duties from the drop-down list.
7. Choose whether or not to make the Virtual WWW site accessible only by trusted hosts (ie. the local network). This way, you can easily host both an intranet and a public web site from the same server.
8. 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 WWW Server* screen displays:

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. Assign a team ID and password to this team.
2. Create a virtual web server. Assign a specific IP address to the virtual web server and choose the AcmeWidgets team as the Webmaster team. Anyone from AcmeWidgets with the proper team ID and password 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.

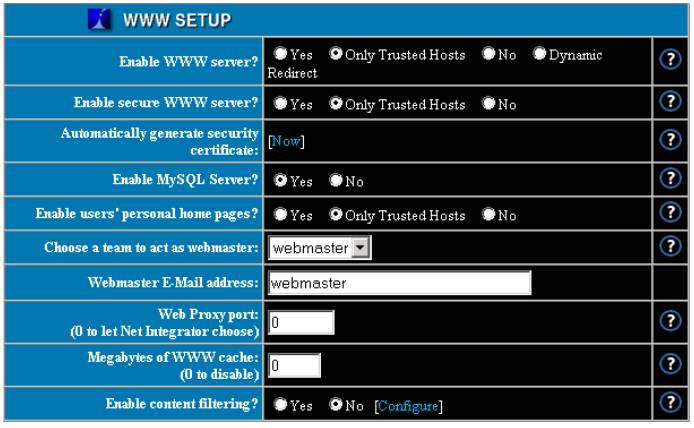
Please Note: If you purchase a security certificate from a certificate authority, delete the file automatically created by Net Integrator and replace it with the one you purchased. You may also want to store a copy of the purchased certificate in a different directory.

Web Caching

In order to save bandwidth, the Net Integrator temporarily stores 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 do this, web caching still functions if your browser is configured this way. However, it you plan use web filtering in conjunction with web caching, all proxy server settings must be removed.

Chapter 12

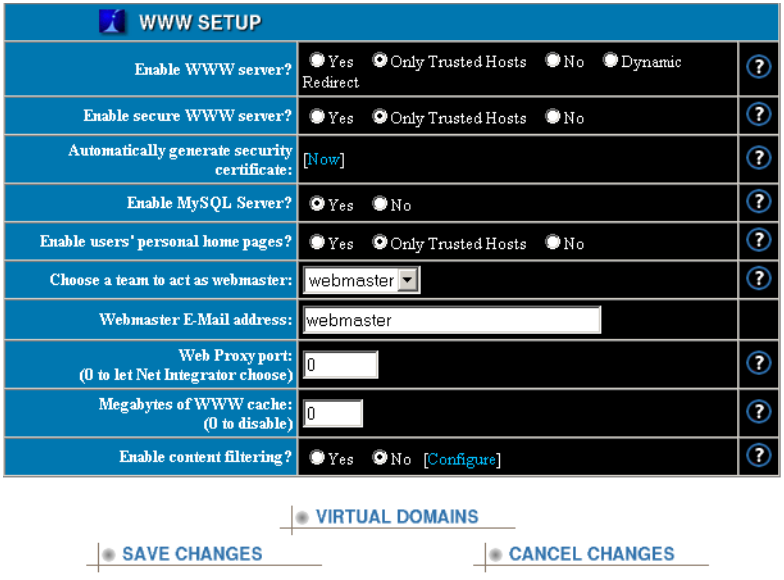
Web Filtering

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.

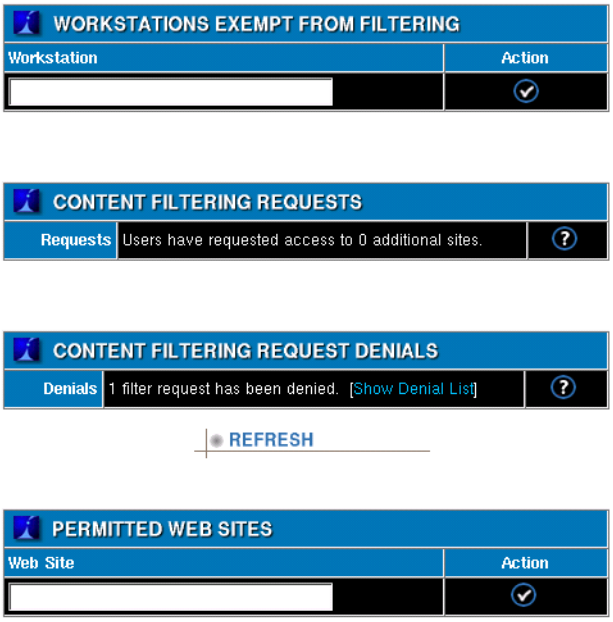
Enabling the Web Filter

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



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:



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 redisplays, and the site displays in the *Permitted Web Site*s 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 redisplays, 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).

Chapter 13

FTP Services

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

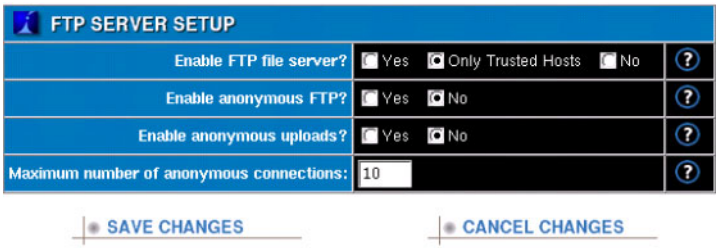
The FTP server can be used in anonymous mode to allow uploads and downloads of files to a specific directory without authentication from the remote user. This anonymous mode of operation is commonly used for public file distribution on the Internet. For example, if your company wants to offer a brochure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

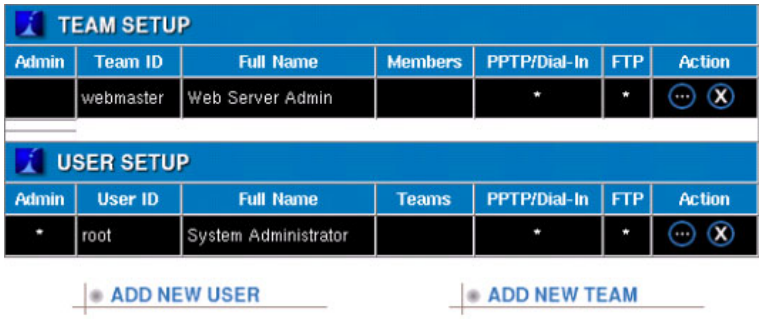
1. Select *FTP* from the *Server Setup* menu on the left side of any WebConfig screen. The *FTP Server Setup* screen displays:



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 overutilization 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:



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.

Chapter 14

Backup & Restore

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 removeable high-capacity hard disk, which provides the following advantages:

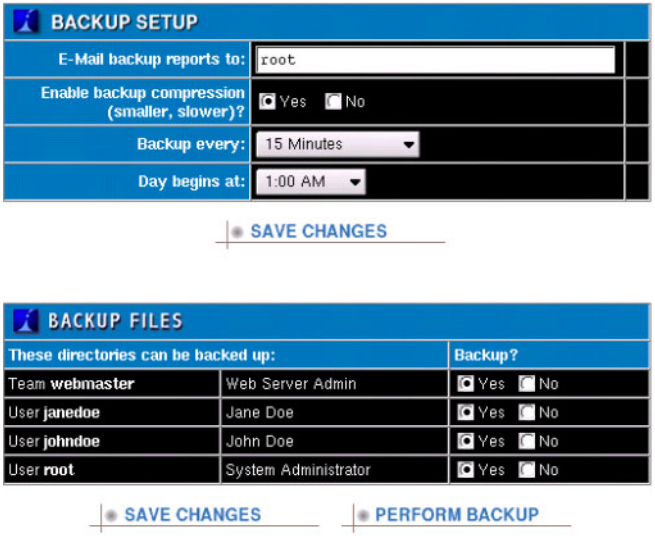
- **Value** – one hard disk costs less than the five backup tapes needed to maintain a tape backup system.
- **High Capacity** – the idb backup cartridge can (in most cases) store a month or more of backup history .
- **Speed** – idb backup matches and often supercedes the backup speeds achieved by the 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. Net Intelligence 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.

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.



2. 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.

3. 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.

4. Select how often you want the system to perform a backup from the drop-down list. The default setting is 15 minutes.
5. 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).
6. 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.
7. Click on the *Save Changes* button to save your selections. The idb system automatically performs the backup procedure.

Initiating an idb Backup

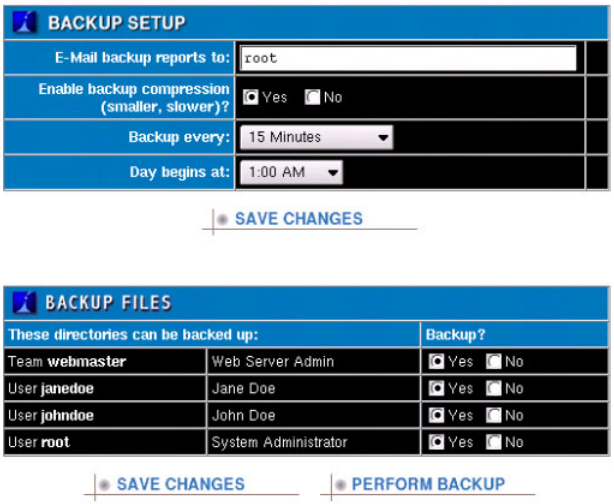
Although the idb system automatically performs backup procedures (without input from a system administrator) you can turn off idb and manually initiate a backup from the control panel (found on the front of the Net Integrator) or from the *Backup* menu (located under the *Server Setup* menu).

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 procedre 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.



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 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. After a complete system restore, all existing files are overwritten with older 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 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 gets overwritten (like with a complete system restore).
    - **Safe Mode Restore –** The contents of a user or team directory gets restored into a new subdirectory called *Restore* (which is created in the useror 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.

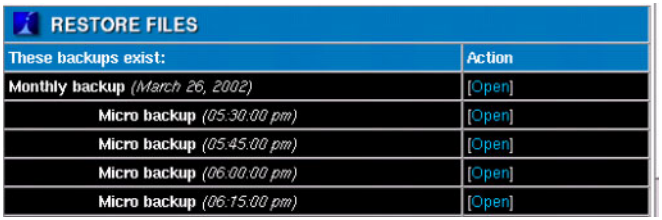
IMPORTANT: Restore procedures can only restore user- and team-level directories. You cannot restore selected files within a directory.

Initiating 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 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):



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).*

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 gets 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 Restore from the Control Panel

IMPORTANT: Inititate 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.

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.

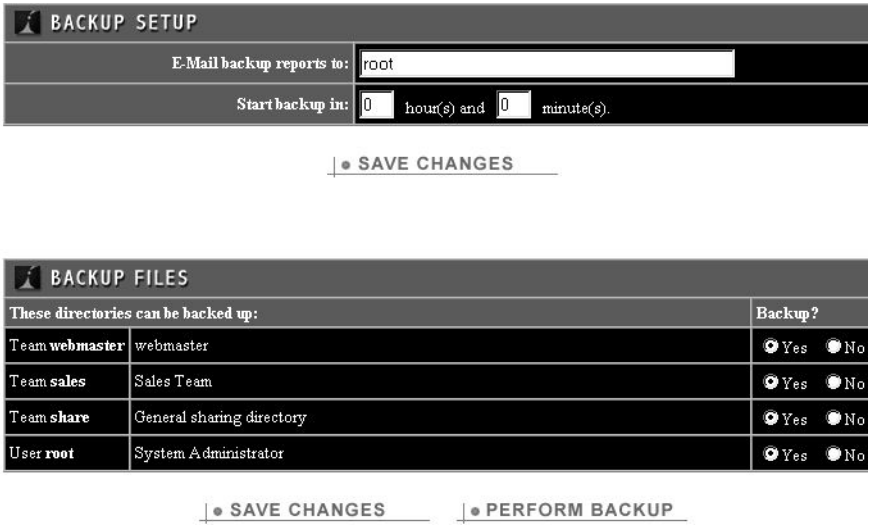
IMPORTANT:A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

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* form 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.



4. 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.

5. Begin a count-down to the backup procedure by entering a time frame in the *Start Backup in* field.
6. 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.
7. 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 gets overwritten (like with a complete system restore).
    - **Safe Mode Restore –** The contents of a user or team directory gets 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.

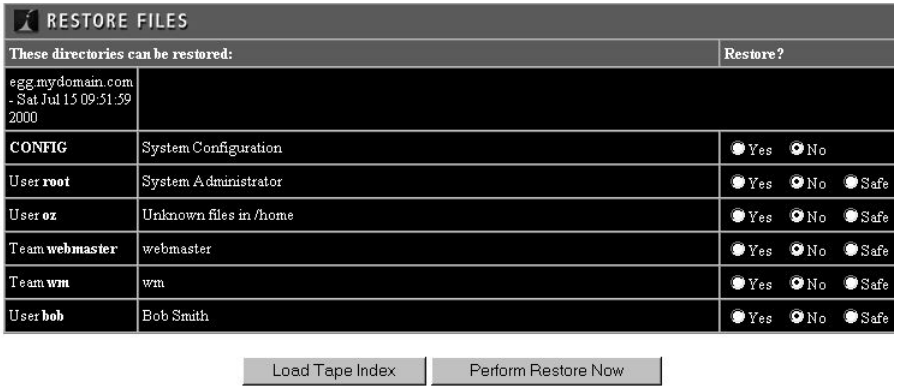
Initiating a Tape Restore

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* form 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.



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 gets 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: Inititate 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.

Chapter 15

Software Update

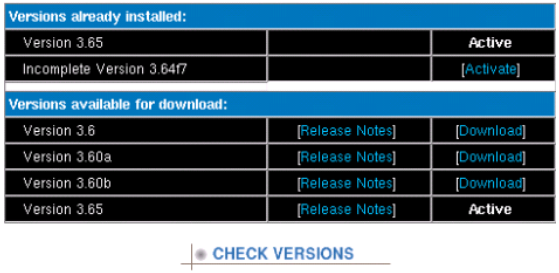
Software Updates

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.

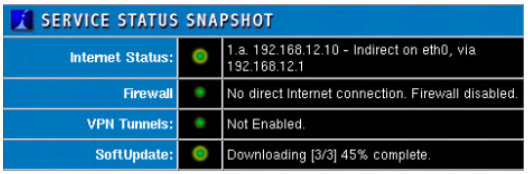
1. Select *Software Update* from the menu on the left side of any WebConfig screen. The *Software Update* screen displays, showing the software version currently running on your Net Integrator and all versions available for download:



2. Click on the *Check Versions* button to update the list of available versions.
3. 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.

4. The new software has to be downloaded to your Net Integrator. To do so, click on the approriate version's *Download* link. The *System Status* screen displays. The *SoftUpdate* line displays the progress of the download:



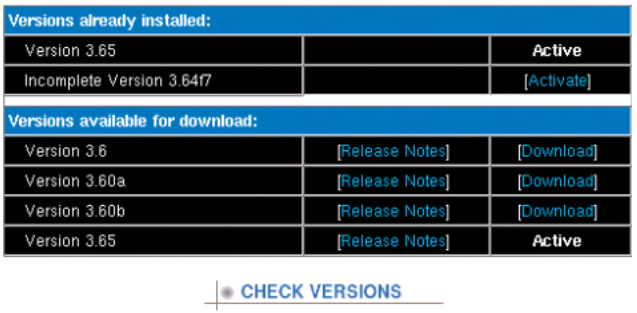
5. When the download is complete, the *SoftUpdate* line reads: *A software update has been installed. To activate it, you must Reboot the Net Integrator.*

6. Click on the *Reboot the Net Integrator* link. The following screen displays:

7. 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.

8. 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:

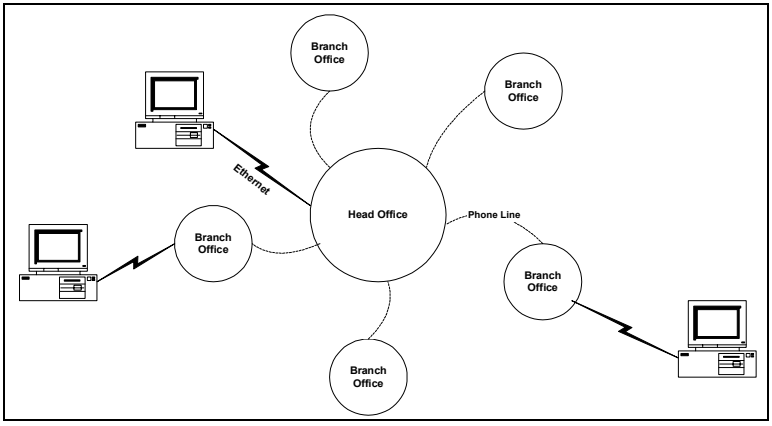


Chapter 16

TunnelVision

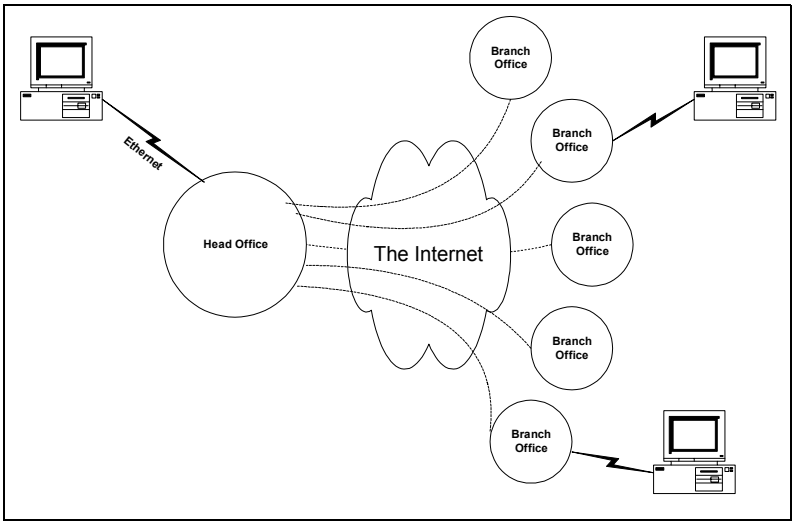
Private Networks

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.

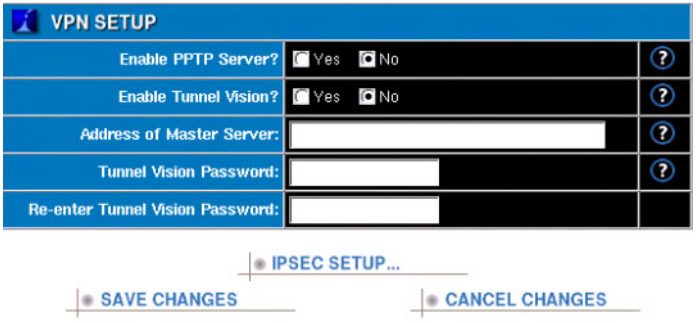
Only one Net Integrator (usually the computer with the fastest Internet connection at your head office) needs to act as the server and have a static IP address. All the others can simply act as clients.

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 19: 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:

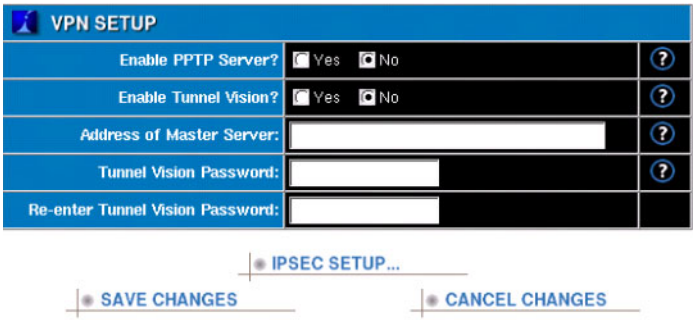


2. Leave the default *Enable PPTP Server* setting.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. Leave the *Address of Master Server* field empty (since the Master server does not initiate connections).
5. Enter a password that the server and client will use to prove to each 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 infomation, 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:



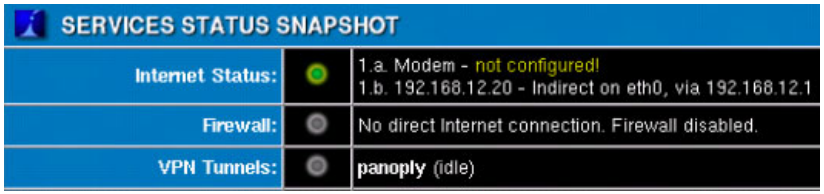
2. Leave the default *Enable PPTP Server* setting.
3. Select *Yes* in the *Enable Tunnel Vision* section of the screen.
4. Enter the Master server's static IP address.
5. Enter the password that was used in step 5 of *Configuring a Master Server.*
6. Re-enter the password to ensure it was entered correctly.
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.



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.

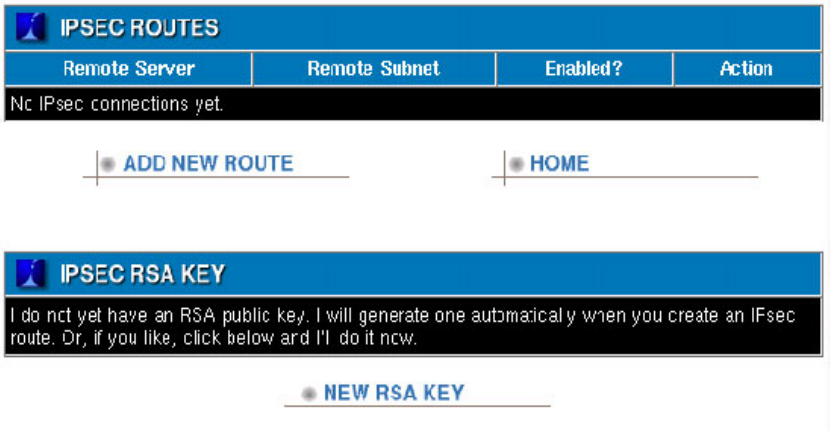
If one end of the tunnel is still on-line, it will try to rebuild the connection automatically. Since this only takes a few seconds and happens only when the tunnel has been idle for a long time, this should not affect you. However, this behaviour can often cause the *VPN Tunnels* status light to turn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

IPsec: An alternative to TunnelVision

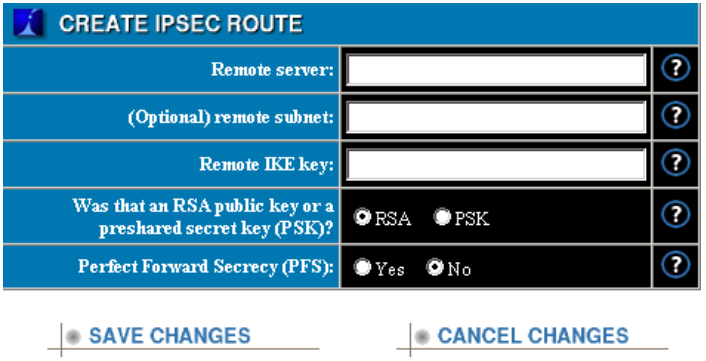
As an alternative to *TunnelVision*, your Net Integrator can create an *IPsec* tunnel to a remote server. *TunnelVision's* more advanced features, such as automatic hostname and route sharing, are not provided by *IPsec*. We generally recommend using *TunnelVision*, however, for strict standards compliance,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

Adding an IPsec route

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



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



3. Enter the IP address (or proper hostname) of the remote server you wish to connect to.
4. To include a private subnet behind the remote server's firewall, enter the subnet here (eg. `192.168.42.0/24`). 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. Obtain the remote server's RSA public key from its administrator and paste it here.

Please Note: It must begin with “0s” for Base-64 formatted keys, or with “0x” for hex formatted keys.

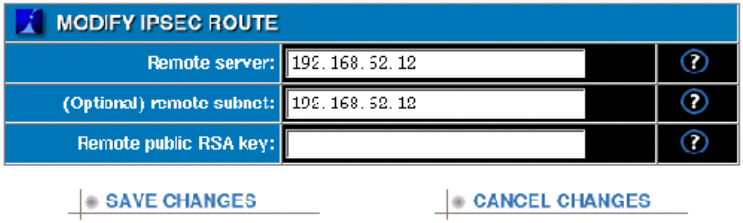
6. Choose to enable or disable Perfect Forward Secrecy (PFS). It must be set the same way on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure to set it correctly.

   With PFS, an attacker who finds out your long-term IKE key still probably cannot read future or past information that you send using the short-term encryption keys that are generated.

   Each IPsec route has a PFS option.
7. 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 . The *Modify IPsec Route* screen displays.



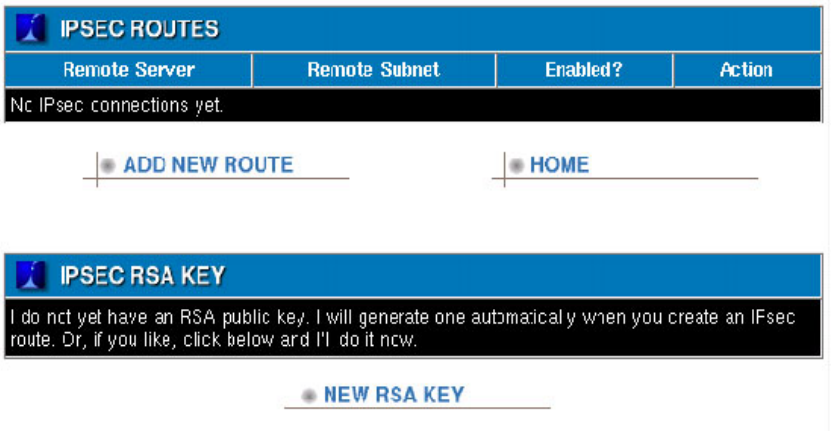
2. Enter the IP address (or proper hostname) of the remote server you wish to connect to.
3. To include a private subnet behind the remote server’s firewall, enter the subnet here (eg. `192.168.42.0/24`). To tunnel only to the remote server, and not to a subnet behind it, leave the *IPsec: Remote Server* field blank, or enter the remote server’s IP address from the first field.
4. Obtain the remote server’s RSA public key from its administrator and paste it here.
5. It must begin with “0s” for Base-64 formatted keys, or with “0x” for hex formatted keys.
6. Click on the *Save Changes button*.

Generating an IPsec RSA Key

This generates an *IPsec* RSA public key you can provide to remote servers you wish connect to. Exchange this key with the remote server's key to create the encrypted tunnel.

Please Note: Net Integrator will automatically generate one when an *IPsec* route is created.

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



2. Generate a new RSA public key by selecting *New RSA Key.*

Chapter 17

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).

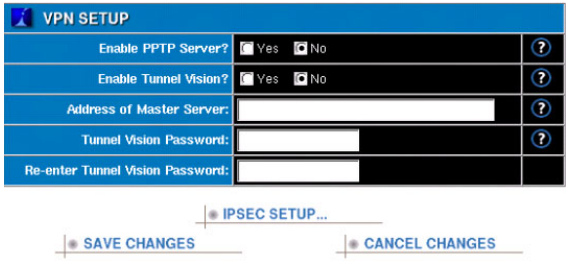
Please Note: Windows has a Point to Point Tunneling (PPTP) client built-in. You have to buy a separate software package if you are using a Macintosh.

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.

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 redisplays. 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.

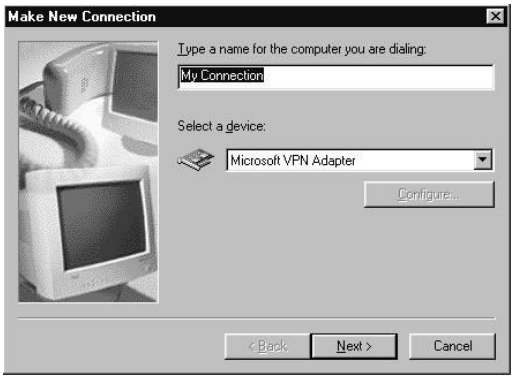
Establishing a VPN Connection

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:

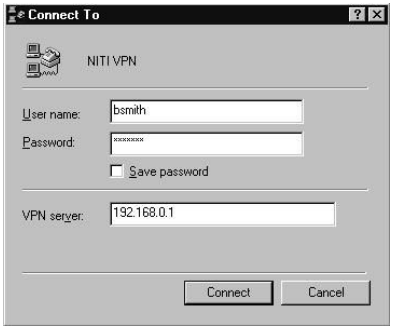


3. Enter a name for the VPN connection. You leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:

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 untrusted 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.

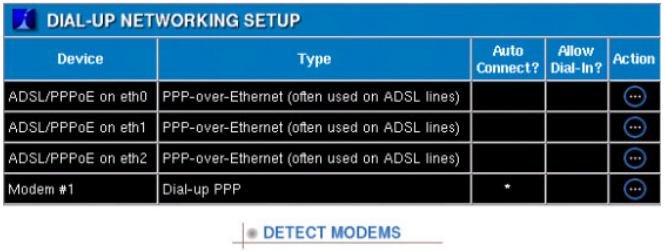
15. You are now connected to your local network through a secure VPN. Depending on your Internet connection, it may take longer than normal to complete network requests. The following icon (showing traffic between your workstation and the Net Integrator you are connected to) displays in the bottom right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

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

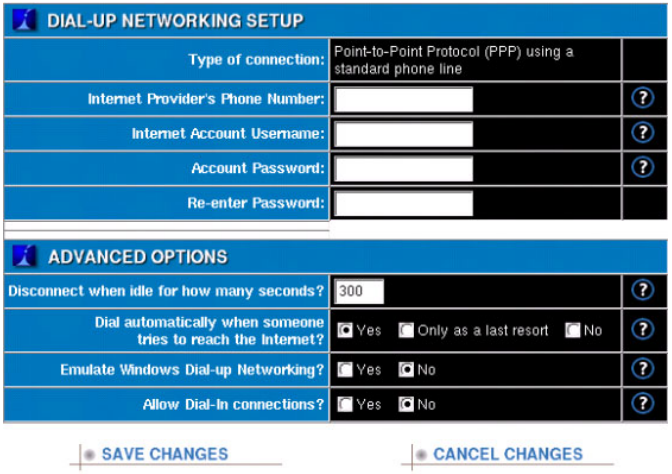
Dial-in Service

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:



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



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 redisplays. 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.

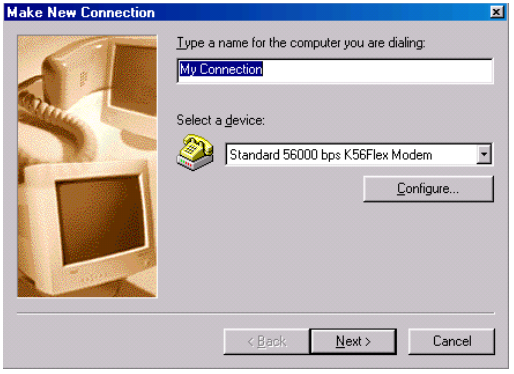
Establishing a Dial-in Connection

When a user dial 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.

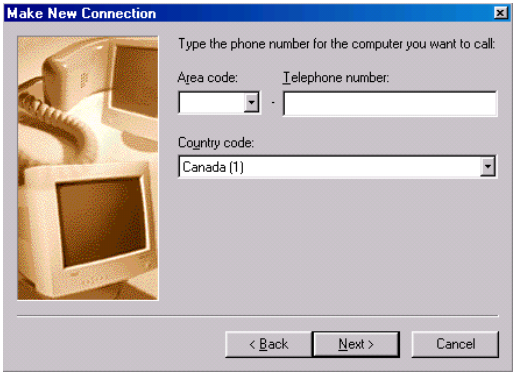
In order to establish a dial-in connection to your network, you need to know your Net Integrator username and password and the phone number of a modem that is connected to an external phone line. Depending on your Internet connection, it may take longer than normal to complete network requests.

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

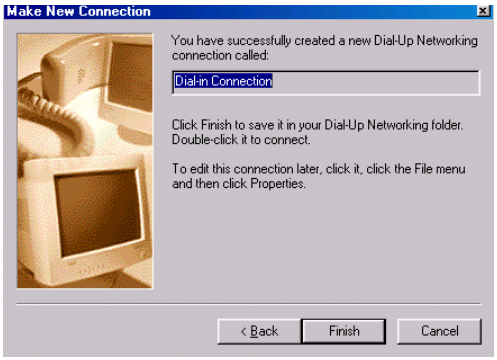
1. From the *Start* menu, select *Programs* > *Accessories* > *Communications* > *Dial-up Networking*.
2. Double-click on the *Make New Connection* icon. The following screen displays:



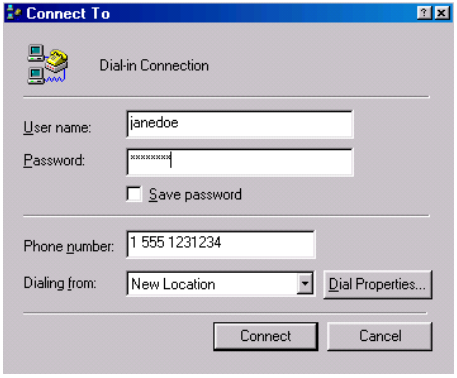
3. Enter a name for the dial-in connection. You can leave the default or use any name that makes sense to you. Click on the *Next* button. The following screen displays:



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.

Chapter 18

Firewall Services

Net Integrator's firewall subsystem is entirely auto-configuring and automatically reconfigures its parameters to adapt to any Net Integrator settings. It's so sophisticated, 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 Certification

Version 3.71 of Net Integrator's operating system is our first candidate for ICSA firewall security certification. 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 non-Remote Administration related access requests from public network clients directed to the following:

- 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 23: 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:

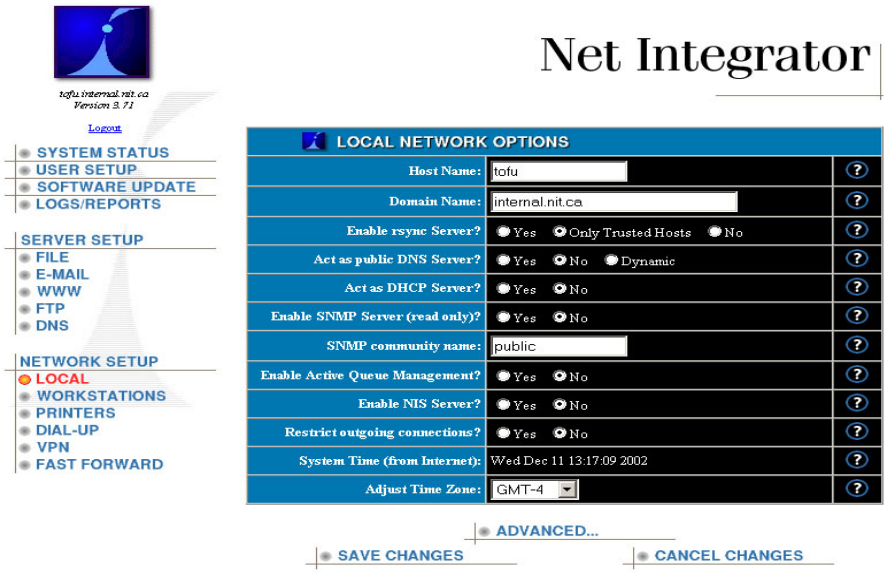
- Telnet (TCP/23) – To access resources on a Unix/Linux computer.
- FTP (TCP/20-21) – To copy files between computers.
- HTTP (TCP/80) – To make web pages available over the Internet.
- HTTPS (TCP/443) – To make secure web pages available over the Internet.
- SMTP (TCP/25) – To transfer or send email 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.

Firewall Log

Please see *Chapter 24: Log Messages* for information on Firewall logs.

Chapter 19

Domain Name Services

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.

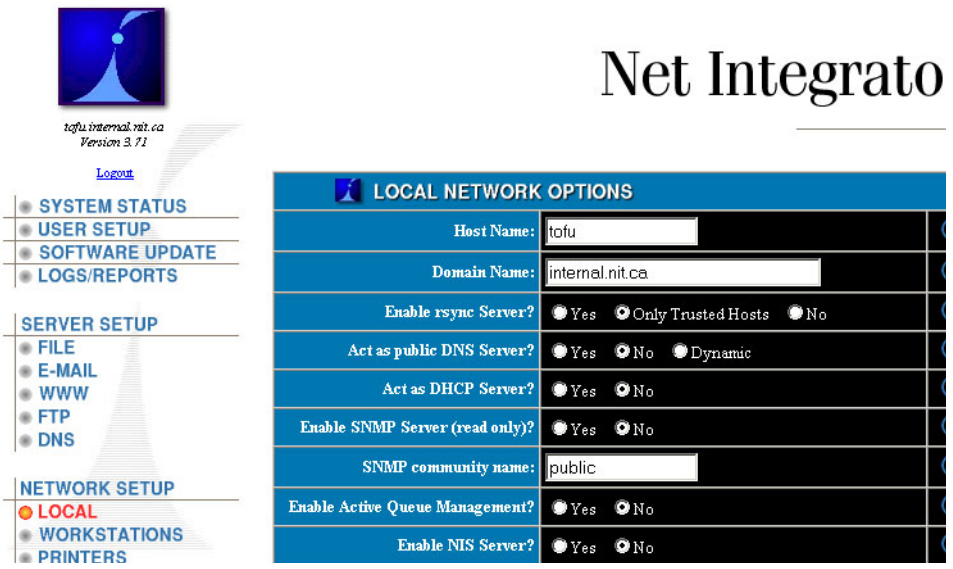
DNS Services

Net Integrator runs two different kinds of DNS services:

- **DNS Lookup and Caching Server –** This server converts domain names (such `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.

Configuring Public DNS

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



2. The default DNS server setting is *No,* meaning that you are not publishing any DNS entries.
    - This option only controls the DNS publishing server and how people outside your local network communicate with it. The DNS publishing server is always active for computers on your local network.
    - If you want to provides services (such as email) to the outside world, you need to enable the DNS server. To do so, select *Yes* **or** *Dynamic*. Your choice depends on some relatively complex issues involved in domain name registration. We will try to explain some of these issues in the following sections.
3. Click on the *Save Changes* button when you have selected the appropriate DNS setting.

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.

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.

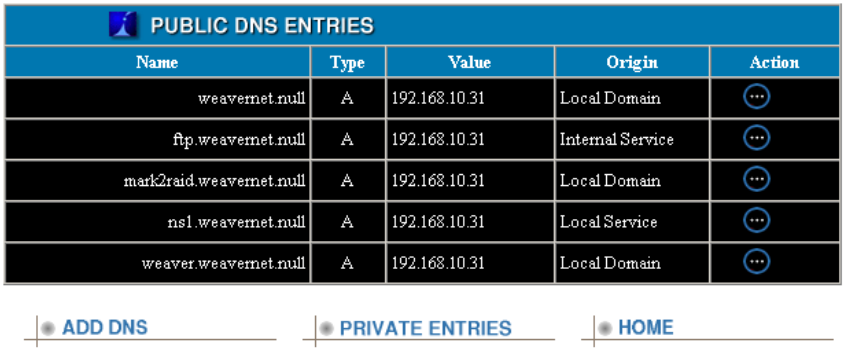
Types of DNS Entries

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:

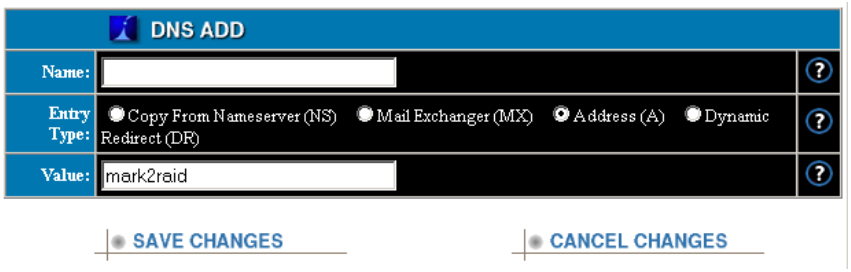


Please Note: To list, create or edit your private DNS entries, click the *Private Entries* button.

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 untrusted (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.

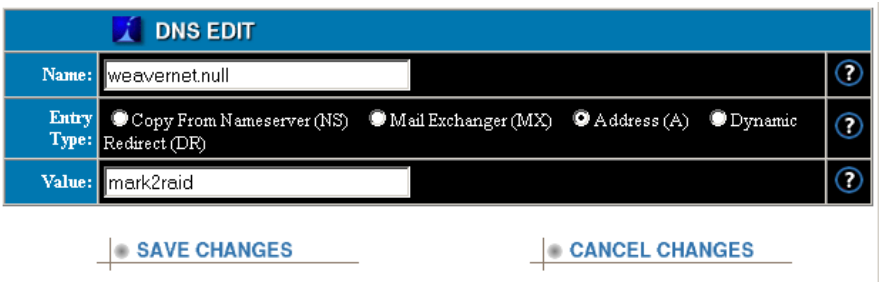
2. Click the *Add DNS* button. The *DNS Add* screen displays:



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:



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

Chapter 20

Workstation Viewer

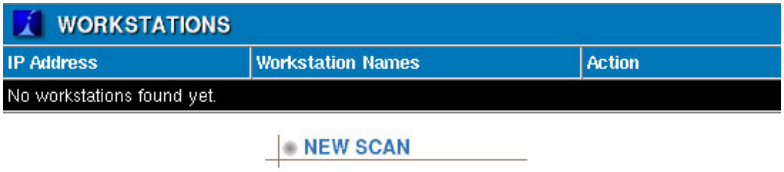
What is the Workstation Viewer?

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 *Network 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:

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

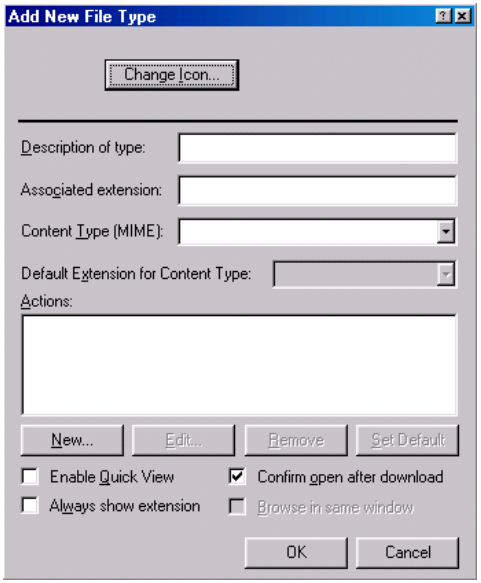
   - `http://download.cnet.com/` (and search for VNC)

Please Note: For the MAC version, go to `http://www.chromatix.uklinux.net/vnc/`

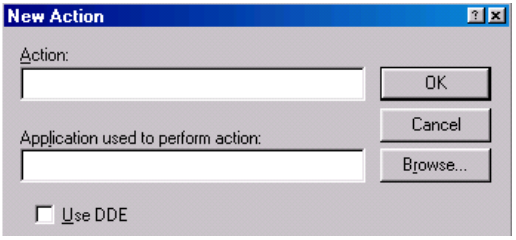
2. The file comes in a zipped format. Unzip the file in a temporary location for installation. Run the Setup program and follow the screens. Accept all defaults during the installation process.
3. When installation is finished, reboot the workstation.
4. From the Start menu, select *Applications > VNC 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 Intenet 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.

Chapter 21

FastForward

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.

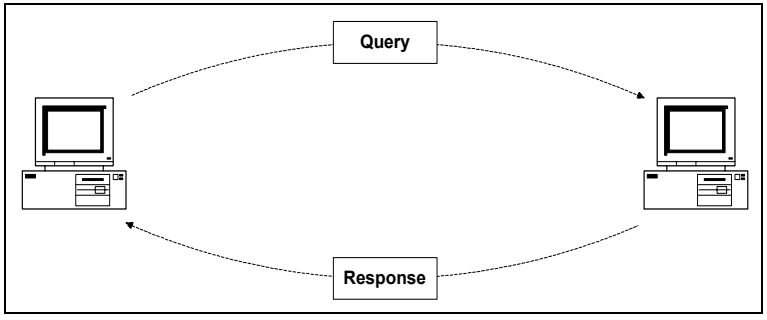
How does a computer know what to do when it receives an IP packet? Somehow, it needs to figure out what service it belongs to, and which open connection it's involved in. For that, it

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.

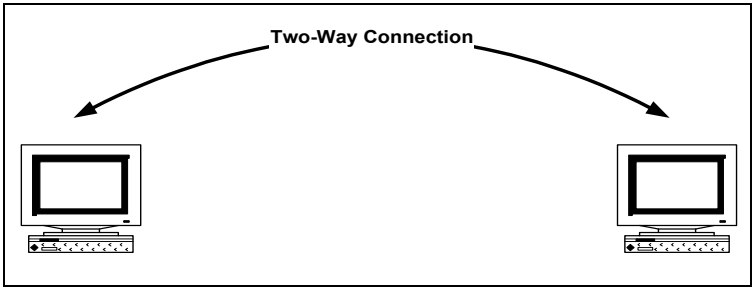
User Datagram Protocol

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

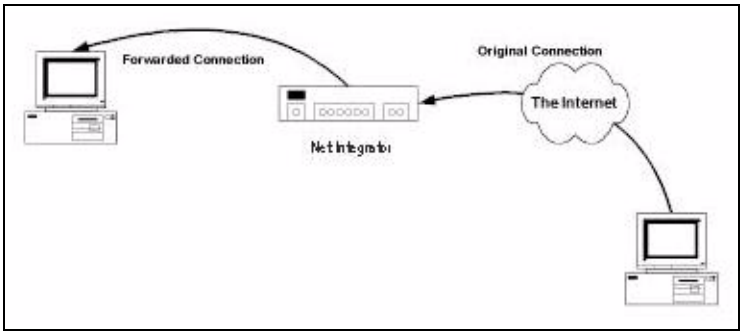
Using TCP is very much like making a telephone call. A person calls you, and you answer. You go through a introductory sequence, you have a conversation, and then you finish the call (or as we say with TCP, you close the connection). TCP is used for more complicated network tasks, like web browsing.



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.

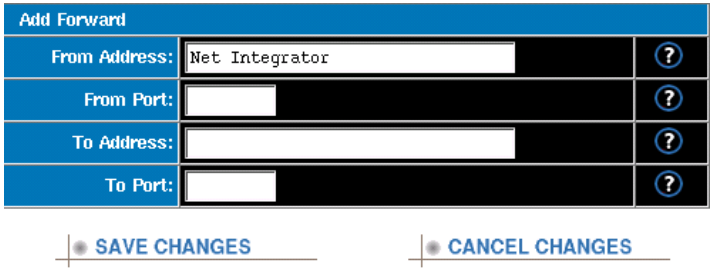
IMPORTANT:Remember that you decrease firewall security when you enable FastForward.

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:



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

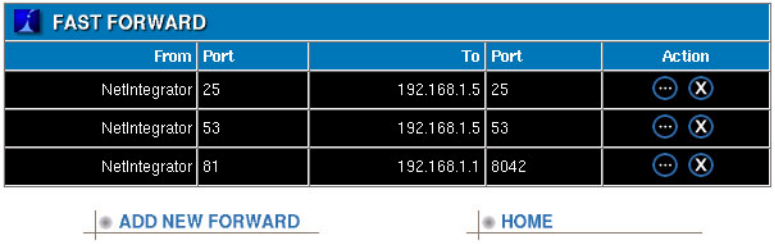
1. On the *Fast Forward* screen, click on the appropriate forward's *Delete Action* button.
2. To confirm the deletion, click on the *OK* button on the window that displays.

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.yournetwork.com:81/`

Here's what FastForward looks like if you choose all three of these settings:



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 24: Log Messages)* shows which Fast Forward entries did and did not work.

Chapter 22

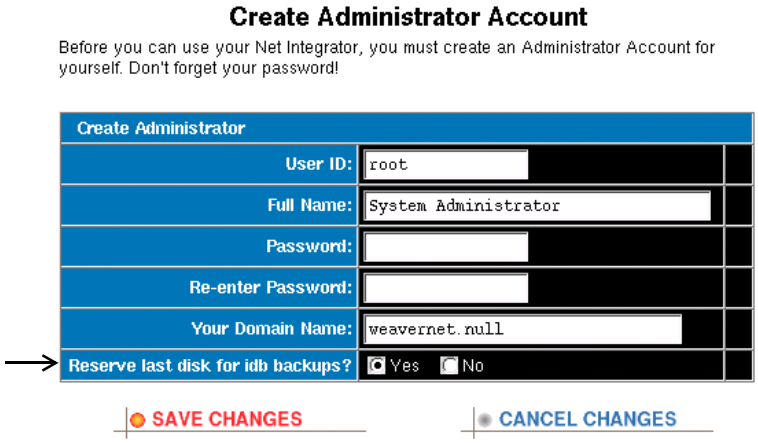
Disk Management

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:



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:

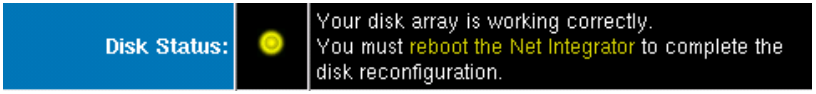
3. When the array has finished building, the following displays in the *Disk Status* section of the screen:

Converting a RAID disk to idb

If your RAID array is working correctly, you can convert a RAID disk to idb.

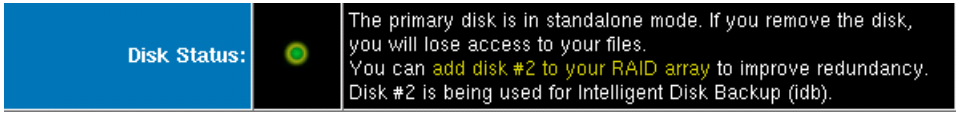
IMPORTANT: Converting your last RAID disk to idb eliminates disk redundancy (regardless of how many disks your Net Integrator has).

1. 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.
2. The following displays in the *Disk Status* section of the screen:



3. Click on the *Reboot the Net Integrator* link. The following screen displays:

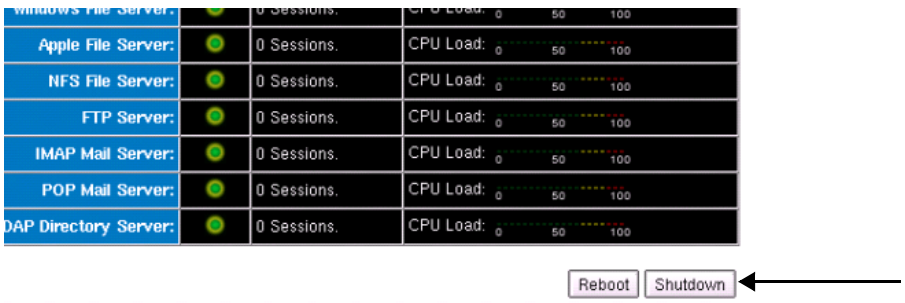
4. When an IP address appears on your Net Integrator's display panel, click on the *Return* button. The *System Status* screen displays. The *Disk Status* section of the screen displays your new disk configuration:



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.

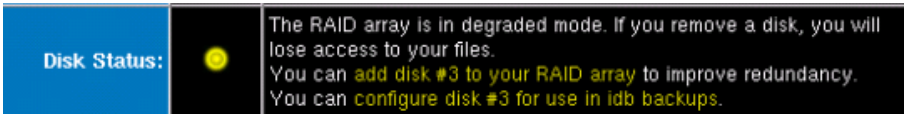
5. *The primary disk is in standalone mode. If you remove the disk, you will lose access to your files.*
   This message displays if have a single disk drive, if you are not using RAID, or if your two-disk RAID array is in degraded mode.
6. *There is no disk available for idb backup.*
   This message 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 unconfigured 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 unconfigured. 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 switch (on the back of the Net Integrator).
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:
   o. Read the IP address on display panel. For demonstration purposes, we will use the following address: `192.168.0.1`
   p. 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 Tape** – 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** – because your hard disk has failed, a new one will be sent to you by Net Integration Technologies. The disk will be sent by overnight courier and should arrive the next morning. 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 power switch (located on the back of the Net Integrator).
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.

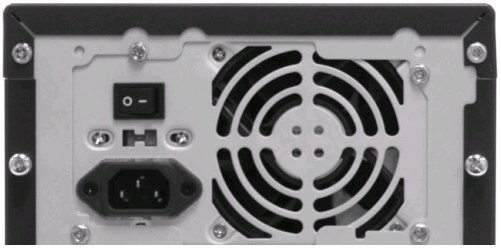

4. Remove the disk from the unit.

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 switch back on



9. Press the power button (on the front of your Net Integrator).
10. When an IP address appears on the the display panel, insert the last backup tape into the tape backup drive.
    Please Note: Skip this step if your last backup tape iss 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.

Chapter 23

MySQL Server

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.)

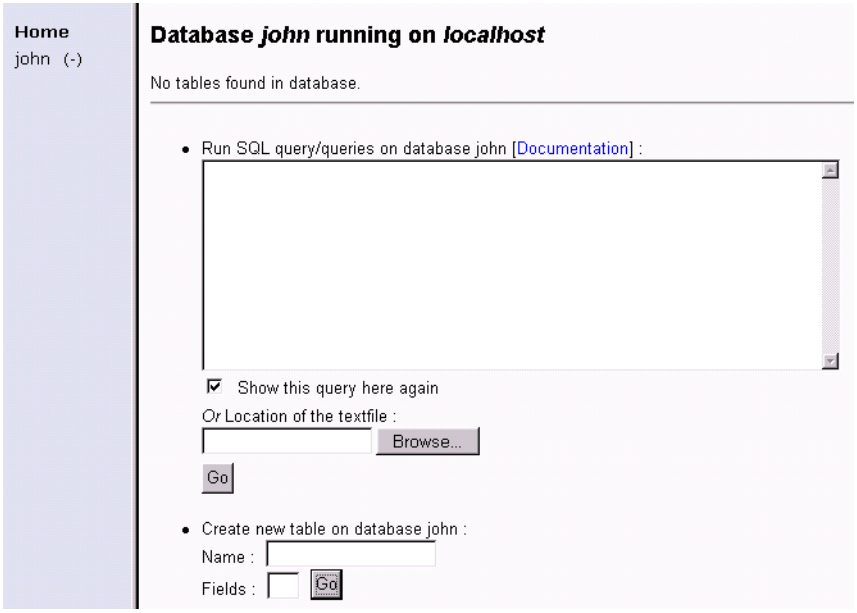
Managing Databases in phpMyAdmin

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*.

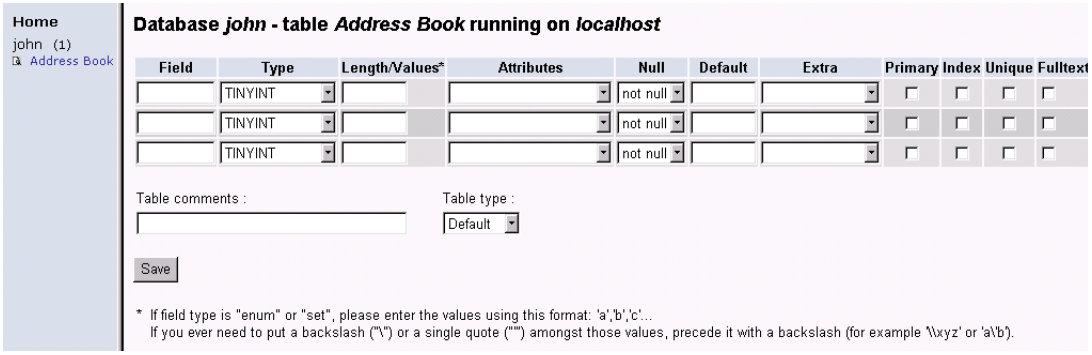
1. Open an Internet browser on your workstation. Newer versions of Netscape or Microsoft browsers are recommended.
2. Read the IP address on your Net Integrator's display panel. For demonstration purposes, we will use the following address: `192.168.0.1`
3. Enter `https://192.168.0.1/mysql` into the browser's address bar. Press *Enter* on your keyboard. Enter your user name and password on the screen that displays.s
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:

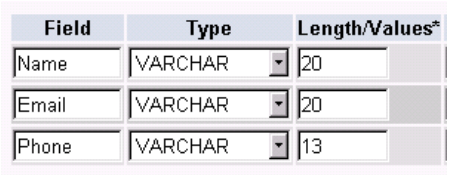


6. To create a new database table, enter the name of the table and the number of fields in the *Create new table...* section of the screen.
   Please Note: The table name cannot contain any spaces.

7. The following screen displays:



8. Enter basic field information.

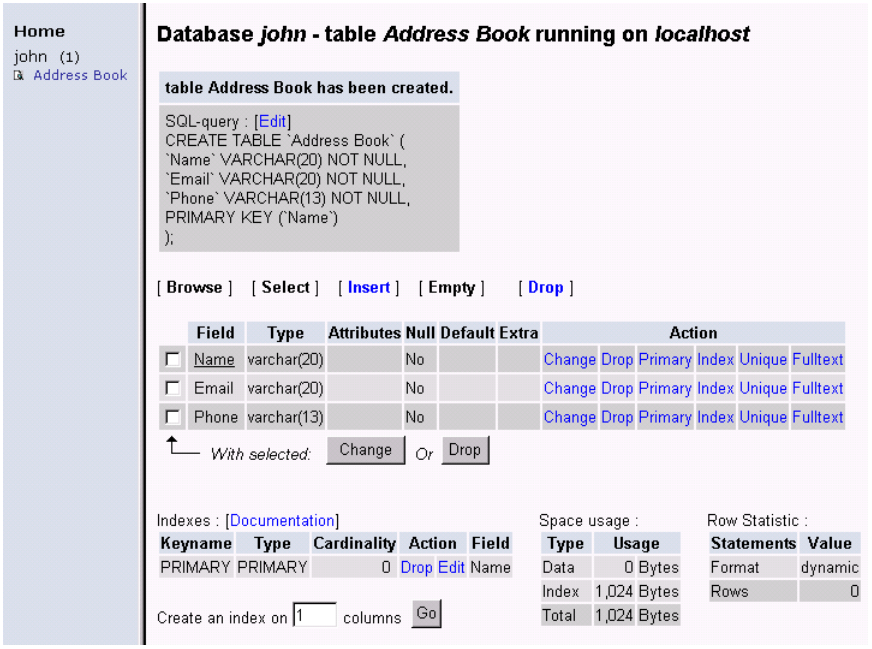


Please Note: *VARCHAR* (in the *Type* column) simply means that the entry contains numerous characters. In the *Length/Values* column, specify the maximum number of characters allowed in the entry.

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.

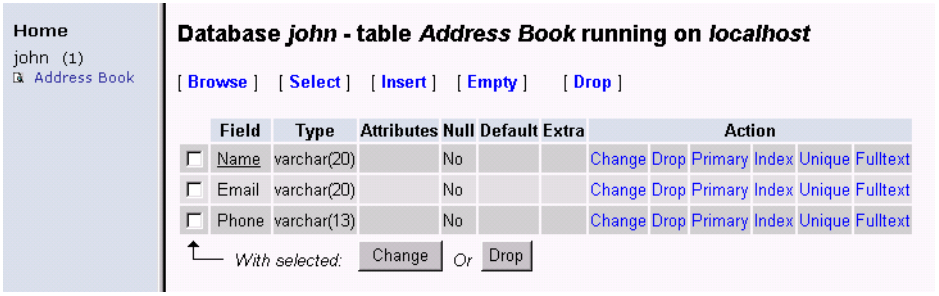
10. Click on the *Save* button. The following screen displays:



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:

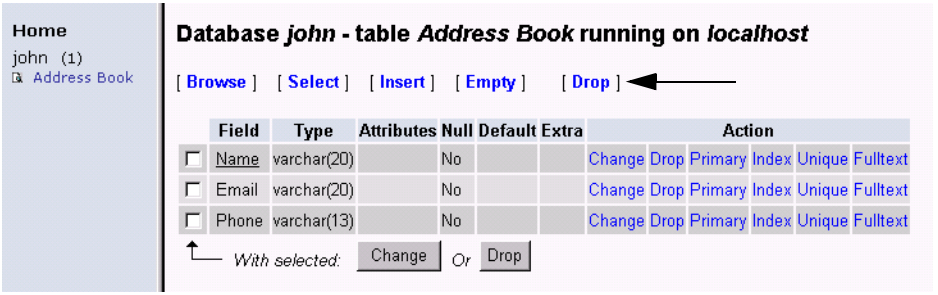


Please Note: This screen has other options not shown in this image.

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.

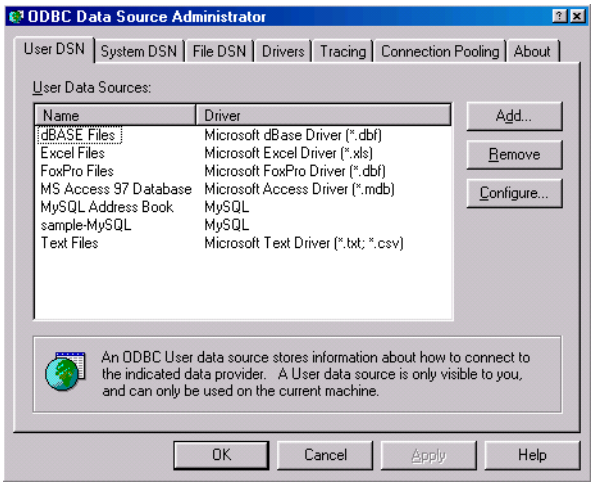
2. Click on the *Drop* button (at the top of the screen).
3. In the window that displays, click on the *OK* button.

Setting up Windows for MySQL Access

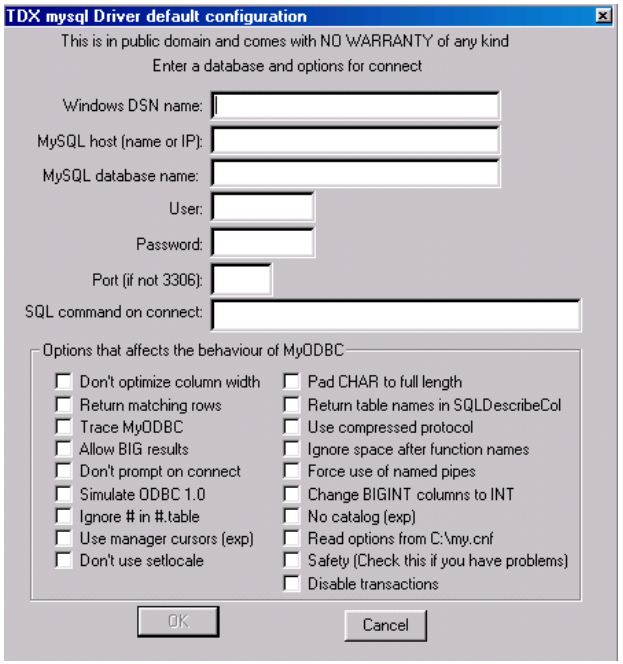
Instead of using phpMyAdmin, you can use *Microsoft Access* to access and manage database tables. We are still using the example of an address book.

1. You first have to download *MySQL ODBC* (Open Database Connectivity). Go to `http://www.mysql.com/downloads/api-myodbc.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:

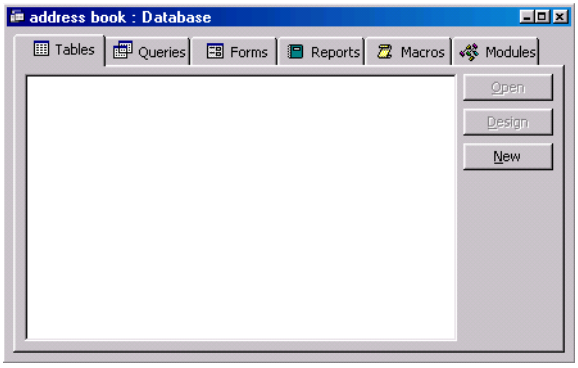
- a Windows DSN Name (such as *MySQL Address Book*)
- your Net Integrator's host name or IP address
- your MySQL database name, user name, and password.

Please Note: You do not have to worry about the other fields on this screen.

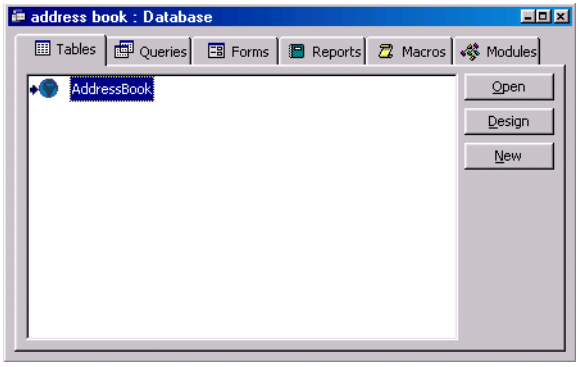
14. Click *OK* on this screen and then on the *ODBC Data Source Administrator* screen.

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 Neighbourhood, 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.

Chapter 24

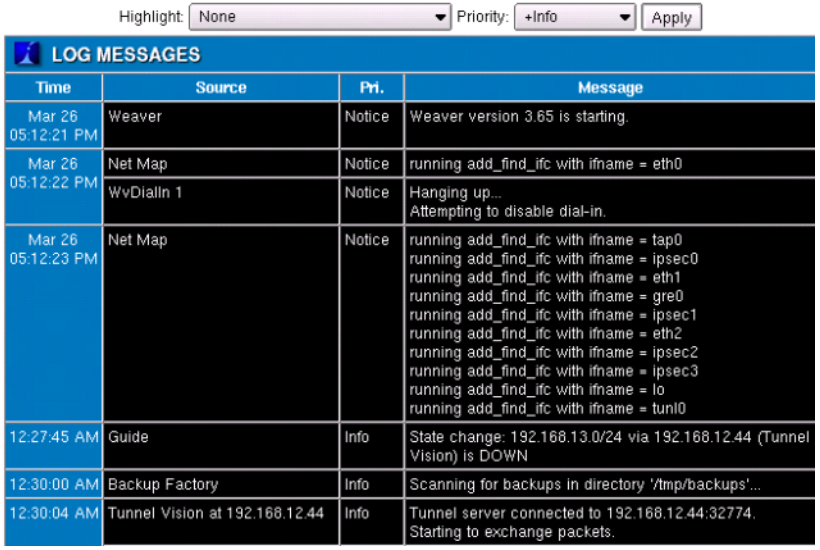
Log Messages

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:



Please Note: Information messages display on a black 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

With ICSA firewall certification, Net Integrator logs requests to send traffic through the firewall. Please see *Chapter 18: 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

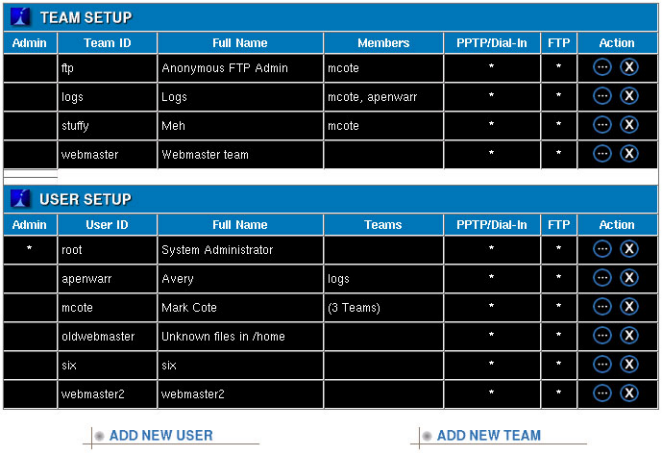
The logs contain the following information:

- 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.)

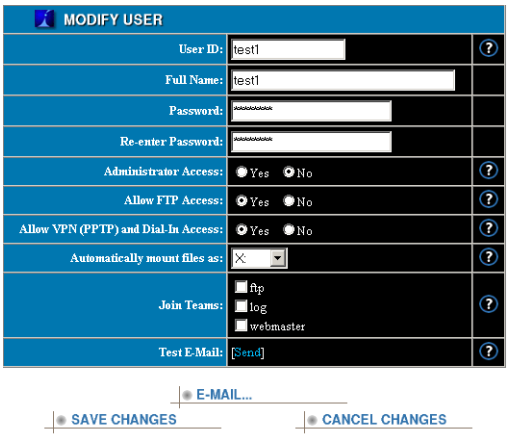
To view the firewall log, you must be a member of the *Logs* team. The firewall log file will then appear in your IMAP folder of your email reader as an incoming message. This team is automatically created by the Net Integrator.

To add a user to the *Logs* team:

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 *Edit Action* button. The *Modify Users* screen displays:



3. Choose the *Logs* team in the *Join Teams* field.
4. Click on the *Save Changes* button.
5. Access your IMAP folder, and the firewall log for the Net Integrator will be one of the incoming emails.

Appendix A

Network File System

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*.

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 JavaScript support.
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 *MySQL* Administration A program used to administer *MySQL* 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 *Strong* or *Medium*).
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 algorithim 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 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 `http://hostname:8042` in the address bar of a web browser. For example, if your Net Integrator's host name is *thunder,* enter `http://thunder:8042` in the address bar.

See *Chapter 2: Connecting to WebConfig* for more information.

WebMail Server A system that allows users to access their email account using any standard web browser.

A

C

D

E

F

N

P

R

S

T

U

V

W