



- Home
- Installation
- Configuration
 - Tutorials
 - Help

My scanner is not working.

When used with multi-function printers that scan and copy, the Wireless **Nd₁** router only supports printing. For bi-directional communication features, such as scanning, connect the multi-function printer directly to the computer. Also, notifications, such as low ink or add paper, are not transmitted from the router to the computer.





- Home
- Installation
- Configuration
 - Tutorials
 - Help

I cannot print to a network printer attached to my router in Macintosh OS 9 or earlier.

Solution 2:

Internet Printing Protocol (IPP) is required to print from a Macintosh computer to a network printer attached to the router. IPP is not supported prior to Macintosh to OS X. Upgrade to Macintosh OS X and refer to [Installing a USB Printer in a Macintosh OS X Environment](#).

[Return to Troubleshooting page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

Tutorials

Below you will find examples of common usage questions and solutions.

Router Settings

[I have purchased another USRobotics Wireless **Nd₁** PC Card or PCI Adapter; what do I do to connect it to the router?](#)

[I have purchased a non-USRobotics Wireless **Nd₁** PC Card, PCI Adapter, or USB Adapter; what do I do to connect it to the router?](#)

[How do I receive System Logs from the router?](#)

[How can I make my wireless network more secure?](#)

[How do I configure my router if I am connecting a gaming console?](#)

[What other router settings may be useful?](#)

[Is the firewall on my router different than the firewall I have running on my computer?](#)

[I did not originally enable any form of encryption when I set up the router in my home, but now I want to secure my wireless network; what do I do?](#)

[I want to connect the router to a DSL router that has an IP address of 192.168.2.1; what do I do?](#)

[I have switched service providers from cable to DSL PPPoE; what do I do?](#)

[I want to be able to access the router remotely on port 8080.](#)

[How do I put my router in Bridge mode?](#)

Parental Control Settings

With your Wireless **Nd₁** Router, you can use the firewall and security settings to set up parental controls for your network to control what types of Internet applications your children can use and even what times of the day they are allowed Internet access.

Before You Set Up Parental Controls

[Have you picked a secure User name and Password for the router?](#)

[Have you set the time on your router?](#)

Parental Control Examples

The examples below show some of the common rules you can implement with the Wireless Nd₁ Router. While these tutorials give specific examples, you can use them and modify the times, dates and other information to apply to your own network.

[I want to control the times when my child's computer can access the Internet.](#)



© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

I want to control the times when my child's computer can access the Internet.

The router comes with two default access control rules under **Internet Access Control** on the [Firewall](#) page to restrict Internet access to computers with IP addresses between the range of 192.168.2.100 and 192.168.2.110. To enable one or both of the rule, select the **On** checkbox for the rule.

- Restrict all Internet access between 10PM and 5PM from Monday to Friday.
- Restrict all Internet access between 12AM and 8AM for the weekend, Saturday and Sunday.

How do I set up a similar rule?

The following rule sets up a time where your child's computer (which has the IP address of 192.168.2.10) is not allowed to access all internet applications during the specified time.

1. Start the router configuration pages by opening a Web browser and typing [192.168.2.1](#)
2. Do one of the following:
 - Assign a static IP address to the computer, in the same subnet as your gateway's management IP address. This must be done on the computer within the network connection settings. The router uses DHCP to assign IP addresses, and depending on your network the computer may get a different IP address and the rules you have created will not apply to the new IP address. It is also recommended to use Static IP addresses which are outside the DHCP Pool of the router.

(For this example, the Default Management IP address for your gateway is 192.168.2.1. The Subnet mask should be 255.255.255.0, and Gateway IP address is 192.168.2.1.)
 - Determine the IP address of the client you want to block from having Internet access by locating the appropriate device listed under **Clients** in the client list on the [Status](#) page (for example, 192.168.2.10).

Clients

Type	Name	MAC Address	IP Address	Expiration
wired	USROBOTI-9FD950	00:0F:FE:3E:08:89	192.168.2.2	58 minutes, 49 seconds

- If you want to set the rule up to apply to multiple computers or devices that are within a select range of IP addresses, you can use that range (for example, 192.168.2.10 to 192.168.2.20).

3. Go to the **Status** page and verify that your router displays the correct Time settings. If the time settings are incorrect, you may need to [set the time](#) on your router.

Device

Name: **USRobotics Wireless Nd1 Router (USR5464)**
 Time: **Monday, August 28, 2006 12:06:39 PM**
 Firmware: **4.81.30.0.2 (Aug 25 2006)**
 Boot loader: **CFE 4.81.30.0.1**
 Printer status: **Not Ready**
 Printer location: **http://192.168.2.1:1631/printers/My_Printer**

4. Click the **Firewall** tab and scroll down to the Internet Access Control area.

Internet Access Control

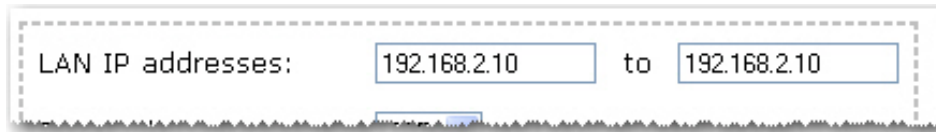
Use this section to deny access to the Internet for certain client devices during specific days and times of the week.

On	LAN IP Addresses	Protocol	Destination Ports	Weekdays	Time Range	
☐	192.168.2.100 to 192.168.2.110	TCP	1 to 65535	Monday to Friday	10PM to 5PM	Delete
☐	192.168.2.100 to 192.168.2.110	TCP	1 to 65535	Saturday to Sunday	12AM to 8AM	Delete

LAN IP addresses: to
 Protocol: TCP
 Port range: to
 Weekday range: Sunday to Sunday
 Time range each day: 12AM to 12AM

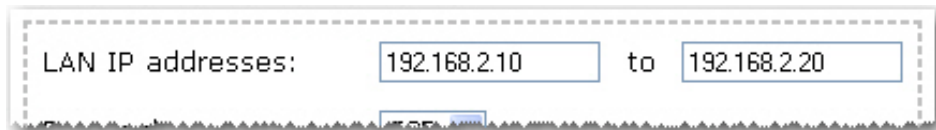
5. Do one of the following:

If you are creating the rule for a single IP address, enter the IP address of the device in both of the **LAN IP addresses** fields. Example: *192.168.2.10* and *192.168.2.10*.

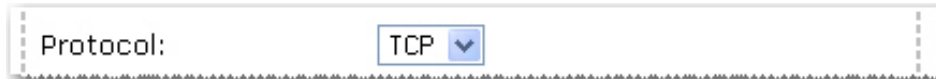


LAN IP addresses: to

If you are creating the rule for a range of IP addresses, enter the range of IP address of the devices in the **LAN IP addresses** field. Example: *192.168.2.10* and *192.168.2.20*.



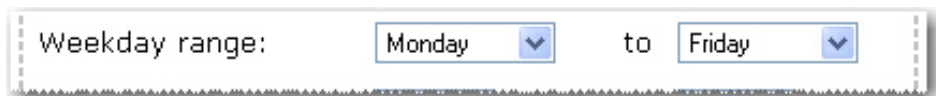
LAN IP addresses: to

6. Select **TCP** as the appropriate **Protocol** for the client.


Protocol:

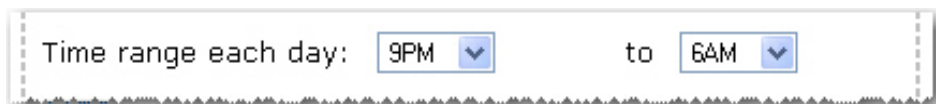
7. The specific port range of 1-65535 will block all Internet access for the client. Enter **1** in the first **Port range** field and **65535** in the second port range field.


Port range: to

8. **To apply the rule for all weekdays:** For **Weekday range**, select **Monday** in the first field and **Friday** in the second field. If you want a different range, you can select different days. If you want the control to be effective for one day, you would select the same day in each field.


Weekday range: to

To apply the rule for weekdays or weekends: You can set up the rules to apply to any range of days, for example Sunday through Thursday night for when your children have school the next morning, and Friday through Saturday for weekend nights when they may be allowed to stay up later. In this case you would need to select **Saturday** and **Sunday** for **Weekday range**, and continue to set up the rule.

9. For **Time range each day**, select **9PM** in the first field and **6AM** in the second field. If you want a different time range, you can make different selections in each field.


Time range each day: to

10. When you are finished, click **Add**.



11. If you want to restrict the access for any additional clients, repeat steps 1 through 10 for each additional client.
12. Click **Save** at the bottom of the page when you are finished. The changes you just made are now in effect.

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

I want to connect the router to a cable modem or DSL router that has an IP address of 192.168.2.1; what do I do?

1. Disconnect your cable modem or DSL router and complete the [installation procedure](#) for the router.
2. When you have finished the installation procedure, start the router configuration pages by opening a Web browser and typing [192.168.2.1](#) and pressing ENTER.
3. Click the [LAN](#) tab.
4. Under **IP Address**, change the IP address of the router to **192.168.3.1** (or whatever IP address you want the router to have) and then click anywhere outside of the IP address field.
5. If you have DHCP Server enabled, it will automatically update the IP range to reflect the change you made to the IP address.
6. Click **Save** at the bottom of the page.
7. You will now need to update the IP address of your computer. You will need to complete this procedure on any computers that were previously connected to the router.

Windows XP, 2000, or NT Users:

- a. Click Windows **Start** and then **Run**.
- b. Type **cmd** and click **OK**.
- c. At the DOS prompt, type **ipconfig /release** and press ENTER.
- d. Then, type **ipconfig /renew** and press ENTER.

Windows Me, 98, or 95 Users:

- a. Click Windows **Start** and then **Run**.
 - b. Type **winipcfg** and click **OK**.
 - c. Click **Release All** and then click **Renew All**.
8. After you have updated your IP information, connect your cable modem or DSL router to the WAN port of the router.
 9. If you need to do any configuration for your cable modem or DSL router, refer to your DSL router documentation. You should now be able to access the Internet and your network resources.

Note: Whenever you need to access the router configuration pages, enter the new IP address that you just configured in Step 4.

[Return to Tutorials page](#)



© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

I have switched service providers from cable to DSL PPPoE; what do I do?

1. Start the router configuration pages by opening a Web browser and typing **192.168.2.1** and pressing ENTER.
2. Select the **Internet** tab.
3. Select your connection type as **DSL modem (also known as PPPoE)** and enter your **User name** and **Password**.
4. You can specify a **Disconnect timeout**. You will then need to specify a timeframe. Selecting and setting a timeframe will cause your Internet connection to be disconnected if your Internet connection is not active for the amount of time you specified.
5. Depending on your DSL ISP, you may need to enter some of the additional information:
 - The **Service Name** of your Internet Service Provider.
 - The **MRU** is the largest packet size the router will allow a computer on the network to receive. MRU stands for Maximum Receive Unit. If your ISP does not instruct you to change this number, leave the default setting of 1492.
 - The **MTU** is the largest packet size the router will allow a computer on the network to send. MTU stands for Maximum Transmission Unit. If your ISP

does not instruct you to change this number, leave the default setting of 1492.

- Select the **Authentication** method that your ISP uses, either **CHAP**, **PAP** or **Automatic**.
 - If your ISP provided you with a host name, enter it in the **Host Name** section.
6. If your ISP requires the use of the MAC address from your Ethernet adapter to identify you on their network, select the correct MAC address from the drop-down menu in the **Clone MAC address** section.

To determine the MAC address of your NIC, complete the following steps:

Windows XP, 2000, or NT Users: Click Windows **Start** and then **Run**. Type **cmd** and click **OK**. At the DOS prompt, type **ipconfig /all**. You will see all of the information regarding your network connection. The MAC address may be listed as the Physical Address.

Windows Me, 98, or 95 Users: Click Windows **Start** and then **Run**. Type **winipcfg** and click **OK**. You will see all of the information regarding your network connection. The MAC address may be listed as the Physical Address.

7. When you have entered all the appropriate information for your connection, click **Save** at the bottom of the page.

[Return to Tutorials page](#)



- Home
- Installation
- Configuration
 - Tutorials
 - Help

I want to be able to access the router remotely on port 8080.

1. Start a Web browser. In the location or address line of your Web browser, type 192.168.2.1 and log in using the user name and password you previously configured in order to access the configuration pages.
2. Click the [Internet](#) tab.
3. Scroll down to the Remote Access section and select the checkbox for **Allow access to this router from the Internet**.

Remote Access

If you want to be able to access your router from outside the LAN, you can enter a port here. You will then be able to access your router through its WAN IP address and that port.

☒ Allow access to this router from the Internet

Port: (must be between 1 and 65535)

Remote address: **http://172.20.66.103:8080**

If you want to be able to access your printer from the Internet, you can select this check box.

☒ Allow access to the print server from the Internet

Remote printer location: **http://172.20.66.103:1631/printers/My_Printer**

4. For **Port**, enter **8080**.

5. Click **Save** at the bottom of the page. Go back to the Remote Access section. You should now see a **Remote address** with a port number at the end separated by a colon. For example, http://154.133.9.24:8080. Write the correct remote address down. You should now be able to log on to the router, through the Internet, from any remote location.

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

I have purchased another USRobotics Wireless *Nd₁* PC Card or PCI Adapter; how do I connect to the router?

SecureEasySetup™ makes it easy to connect wireless clients to your wireless router. SecureEasySetup automatically configures wireless security settings between your router and your wireless clients.

Note: While the router is in SecureEasySetup configuration mode, you can only configure one SecureEasySetup device at a time. Attempting to connect multiple devices may result in errors.

1. [Install your router.](#)
2. Install your PC Card or PCI Adapter.
3. Press the **SecureEasySetup** button on your router for 1 second. The SecureEasySetup LED will blink, indicating that it is ready to connect a SecureEasySetup device.
2. Press the **SecureEasySetup** button in the utility for your wireless adapter.

Your wireless adapter utility will display a message when the connection has been successfully completed.

The SecureEasySetup LED on your router will stop blinking when the SecureEasySetup process has completed on the router.

[Return to Tutorials page](#)



© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

I have purchased a non-USRobotics Wireless Nd1 PC Card, PCI Adapter, or USB Adapter; what do I do to connect it to the router?

1. Start a Web browser. In the location or address line of your Web browser, type **192.168.2.1** to access the router configuration pages.
2. Go to the **Status** page to view your current wireless security settings.

Wireless

Wireless:	Enabled
Network name:	USR5464
Broadcast name:	Enabled
MAC address:	00:14:A5:96:70:49
Mode:	Access Point
WDS restrictions:	Disabled



3. Refer to the documentation for your new wireless PC Card, PCI Adapter, or USB Adapter to determine when and where you will need to enter the wireless and security settings for the router.
4. After you have entered the correct settings and saved the information, you should be able to establish a wireless connection with the router.

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

How do I receive System Logs from the router ?

1. Start you Web browser.
2. In the location or address line, type: **192.168.2.1** and press ENTER to access the router configuration pages.
3. Enter your user name and password and click **LOGIN**.
4. Click the **Log** tab.

Note: You will need to have a syslog daemon utility using UDP over port 514 installed on the target computer in order to view the system logs. You should now be able to receive System Logs at the specified location.

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

I did not originally enable any form of encryption when I set up the router in my home, but now I want to secure my wireless network; what do I do?

1. Start the router configuration pages by opening a Web browser and typing 192.168.2.1
2. Go to the [Security](#) page and look for your **Wireless** settings.
3. [Select a Wireless Method from the drop-down menu](#) and enter the appropriate information.
4. When you are done selecting these options, click **Save** at the bottom of the page.
5. Enable the appropriate encryption option and enter the encryption settings on each wireless client in your network. If you do not enter the correct settings, that wireless client will not be able to access the router.

You should now have a secured wireless network. If you experience any difficulties, refer to the [Security](#) section in this User Guide for more detailed information about the Security settings.

[Return to Tutorials page](#)





© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

Have you picked a secure User name and Password for the router?

You want to have a secure User name and Password for the router to restrict access to the router settings.

1. Access the router configuration pages by opening a Web browser and typing **192.168.2.1** and pressing ENTER.
2. Enter your Login and password when prompted, then press Ok.
3. Click the **Security** tab. Your current user name and password are displayed on the page.
4. To change your user name and/or password, enter the new user name and password and click **Save** at the bottom of the page. You will need to log in to your router with the new user name and password.

Password Rules:

1. The Wireless **Nd₁** Router lets you set a password up to 15 characters long. The most secure passwords are usually between 8 and 15 characters long.

2. The router will allow you to enter a space or other punctuation in your password.
3. Use a mixture of upper (**A** through **Z**) and lower (**a** through **z**) case letters.
4. Adding numbers **0** through **9** to a password increases security.
5. Use ASCII symbols, such as ~ ! @ # \$ % & ^ *, etc, to further increase the security of your password.

[Return to Tutorials page](#)



- Home
- Installation
- Configuration
 - Tutorials
 - Help

How do I put my router in Bridge mode?

Bridge Mode is used to connect two isolated networks wirelessly. If this feature is enabled, wireless clients will not be able to connect to the router. Bridging is used if you are trying to connect two networks or two groups of wired clients, each with its own router or wireless access point, that cannot be conveniently connected using Ethernet cabling. An example of this type of situation would be two homes that want to share network resources without running cabling through their yards.

Note: In Bridge mode, the Wireless Nd₁ Router does not support [Wi-Fi Multimedia \(WMM\)](#).

1. Access the router configuration pages by opening a Web browser and typing [192.168.2.1](#) and pressing ENTER.
2. Enter your Login and password when prompted, then press Ok.
3. Click the [Wireless](#) tab.
4. Scroll down to the **Bridge Mode** section.

Bridge Mode

Bridge mode is used to connect only to another access point. In bridge mode, wireless client devices cannot connect to the router. If you enter the MAC addresses of bridging devices in the WDS Restrictions table, only those devices will be permitted to connect to the router. Please note that any WDS device you will connect to must use one of the following security methods: WPA (PSK) with AES, WPA (PSK) with TKIP, WEP or None.

☐ Bridge mode

5. Select **Bridge mode**.

6. To allow wireless clients to connect to the network while the router is in Bridge mode, scroll down to the WDS Restrictions section.



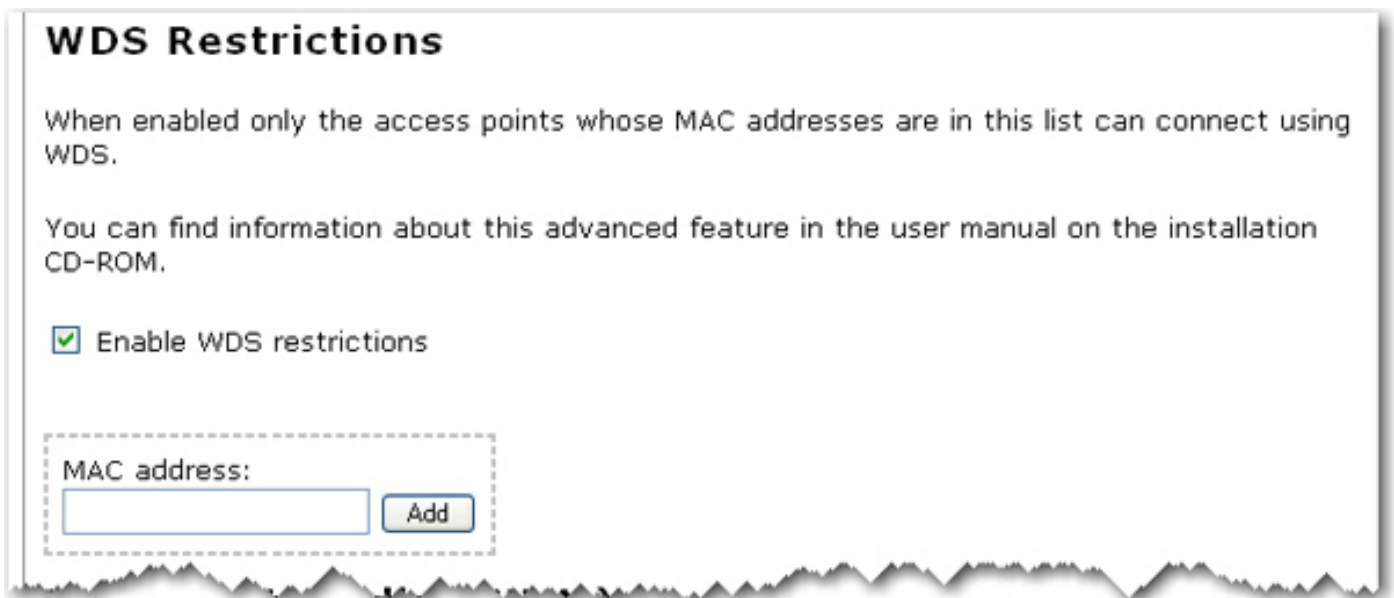
WDS Restrictions

When enabled only the access points whose MAC addresses are in this list can connect using WDS.

You can find information about this advanced feature in the user manual on the installation CD-ROM.

☐ Enable WDS restrictions

7. Select **Enable WDS restrictions**.
8. Enter the MAC addresses of the wireless routers or access points that will connect to this router and click the **Add** button.



WDS Restrictions

When enabled only the access points whose MAC addresses are in this list can connect using WDS.

You can find information about this advanced feature in the user manual on the installation CD-ROM.

☒ Enable WDS restrictions

MAC address:

If your router is set with one of the following security methods and encryption types, all WDS connections to the router should use **WPA-PSK (TKIP)**:

- **WPA2-PSK (TKIP and AES)**
- **WPA2-PSK (TKIP)**
- **WPA-PSK (TKIP and AES)**

- **WPA-PSK (TKIP)**

If your router is set with one of the following security methods and encryption types, all WDS connections to the router should use **WPA-PSK (AES)**:

- **WPA2-PSK (AES)**

- **WPA-PSK (AES)**

In both of these case, the **Pass phrase** (which is also commonly called a *Network key*, *key*, or *Personal shared key*) you entered for the wireless security on your router will be also used as the Personal Shared Key (PSK) for WDS connections. However, all wireless clients connecting to the router should continue to use the same security method and encryption type that you configured on your router.

9. Click **Save** to apply all your new settings and reboot the router after you have completed all your changes.

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

How can I make my wireless network more secure?

Select the most secure wireless security method and encryption type.

For your wireless security settings, it is recommended that you select the **WPA2 and WPA (PSK)** wireless security method using **TKIP and AES** encryption for the most secure wireless network.

To see what wireless security settings you have applied on your router, start a Web browser. In the location or address line of your Web browser, type **192.168.2.1** and log in using the user name and password for the router. Your wireless security settings are displayed under **Security** on the **Status** page.

Restrict devices that are allowed to connect to the router.

Why?

Restricting your wireless network to only specified devices means that any other wireless devices within range of your network will not be allowed to connect, even if they crack your user name and password. This protects the computers on your network, and also assures that all the bandwidth on your network is available to your devices.

How?

Use *MAC Address filtering* to restrict the devices that can connect to your wireless network. The Media Access Control address (MAC address), is a unique identifier that is assigned to computer hardware (desktops, laptops, routers, gaming consoles, etc.). Your router can use this identifier to [allow only specific devices](#), or even [deny a specific device](#) if you have noticed another user connected to your wireless network.

Password Security

To protect your wireless network, use the following rules for guidelines on creating a strong password:

1. The Wireless **Nd₁** Router lets you set a password up to 15 characters long. The most secure passwords are usually between 8 and 15 characters long.
2. The router will allow you to enter a space or other punctuation in your password.
3. Use a mixture of upper (**A** through **Z**) and lower (**a** through **z**) case letters.
4. Adding numbers **0** through **9** to a password increases security.
5. Use ASCII symbols, such as **~ ! @ # \$ % & ^ ***, etc, to further increase the security of your password.

[Return to Tutorials page](#)



© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

What other router settings may be useful?

In addition to your Internet connection settings, there are advanced settings and features on your Wireless **Nd₁** Router that you may find useful.

Set the Time on your router.

Why?

Setting the time on your router assures that system logs will generate useful information so you can track system events. Also, if you are setting up any parental controls or firewall rules, you must set the time to be sure that the rules will be applied correctly.

How?

You can set your [Time settings](#) from the [Device](#) page.

Create a backup of your router settings.

Why?

In the event of a device failure or if you need to restore to the factory default settings of your router, you can restore your settings from the backup and you will not have to re-enter all of your settings. If you have parental control rules or firewall settings for specific gaming devices or applications, this can save a lot of time in getting your full network up and functioning.

How?

Create a backup: To create a backup of your router settings, go to the [Device](#) page and [follow the instructions](#).

Restore from a backup: To restore your router settings from a backup file, go to the [Device](#) page and [follow the instructions](#).

Check for updates for your router.

Why?

Updates may be available for your router. These firmware updates can provide new and added features to your router, and in some cases even fix performance issues some users may have. It is a good idea to check for updates after you have initially installed

and configured your router, and also to check for updates on a regular basis.

How?

To check for updates for your router, go to the [Device](#) page and [follow the instructions](#).

[Return to Tutorials page](#)





- Home
- Installation
- Configuration
 - Tutorials
 - Help

Is the firewall on my router different than the firewall I have running on my computer?

Yes. If you have firewall software running on your computer, it is different than the firewall on your router.

The settings on the firewall software on your computer apply only to your computer. The firewall settings for the router apply to your entire network.

Also, if you have had to configure your firewall software on your computer to opening specific ports for Internet based games or applications, VPN clients, VoIP services, etc., they may also need to be opened on your router. See the documentation for the application or service to determine if you need to set any [Port Forwarding](#) or [Port Triggering](#) settings on your router.

[Return to Tutorials page](#)





© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

How do I configure my router if I am connecting a gaming console?

If you want to connect a gaming console to your router, such as a Microsoft Xbox® or Sony PlayStation2™, you will have to use open up access to specific ports so the devices can communicate with the Internet. This is done from the [Firewall](#) page, using **Port Triggering**.

The router comes with a default Port Triggering rule that you will need if you are connecting a Sony Playstation2™ that needs to access the Internet to your router. To enable the rule, select the **On** checkbox for the rule. This page also details how you could create your own [PlayStation2™ Port Triggering rule](#).

Note: Opening ports on a router can cause potential security risks. In particular, opening Terminal Services UPnP Port 3389 on Windows XP can allow Internet hackers to take over your computer if Windows XP is not patched with Microsoft's latest security updates. If you are opening ports on your router, you will want to make sure you have wireless security applied to the router, and you may want to restrict the devices that are allowed to connect to the router to ensure a secure wireless network.

The following is an examples on how to configure your router if you are connecting a Xbox®. For a complete list of applications and port information, visit www.iana.org.

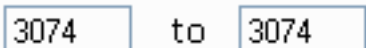
Create Port Triggering rules for an Xbox®

The following rules give the example for an Xbox, where you need to open the TCP port 3047 and UDP ports 88 and 3047 on your router. To create a similar rule, you will need to know which TCP and UDP port(s) need to be opened so the device can communicate over the Internet.

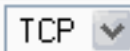
1. Start a Web browser. In the location or address line of your Web browser, type **192.168.2.1** and log in using the user name and password you previously configured in order to access the configuration pages.
2. Click the **Firewall** tab.
3. Scroll down to the **Port Triggering** section.
4. Select **TCP** for the **Outbound protocol**.

Outbound protocol: 

5. For **Outbound port range**, enter **3074** in both boxes.

Outbound port range: 

6. Select **TCP** for the **Inbound protocol**.

Inbound protocol: 

7. For **Inbound port range**, enter **3074** in both boxes.

Inbound port range: to

8. For **Destination port range**, enter **3074** in both boxes.

Destination port range: to

9. Click **Add**.

Add

On the page, you should see the rules for TCP port 3074.

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☒	TCP	3047 to 3074	TCP	3074 to 3074	3074 to 3074	Delete

10. Next, select **UDP** for the **Outbound protocol**.

Outbound protocol:

11. For **Outbound port range**, enter **88** in both boxes.

Outbound port range: to

12. Select **UDP** for the **Inbound protocol**.

Inbound protocol:

13. For **Inbound port range**, enter **88** in both boxes.

Inbound port range: to

14. For **Destination port range**, enter **88** in both boxes.

Destination port range: to

15. Click **Add**.

Add

On the page, you should see the rules for UDP port 88.

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☒	TCP	3047 to 3074	TCP	3074 to 3074	3074 to 3074	Delete
☒	UDP	88 to 88	UDP	88 to 88	88 to 88	Delete

16. Select **UDP** for the **Outbound protocol**.

Outbound protocol:

17. For **Outbound port range**, enter **3074** in both boxes.

Outbound port range: to

18. Select **UDP** for the **Inbound protocol**.

Inbound protocol: UDP

19. For **Inbound port range**, enter **3074** in both boxes.

Inbound port range: 3074 to 3074

20. For **Destination port range**, enter **3074** in both boxes.

Destination port range: 3074 to 3074

21. Click **Add**.

Add

On the page, you should see the rules for UDP port 3074.

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☒	TCP	3047 to 3074	TCP	3074 to 3074	3074 to 3074	Delete
☒	UDP	88 to 88	UDP	88 to 88	88 to 88	Delete
☒	UDP	3074 to 3074	UDP	3074 to 3074	3074 to 3074	Delete

22. Click **Save** at the bottom of the page when you are finished.

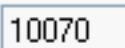
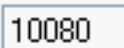
Create Port Triggering rules for a PlayStation2™

Even though the router comes with the default rule for enabling Port Triggering for a PlayStation2™, the following steps show how you could create the rule yourself.

1. Start a Web browser. In the location or address line of your Web browser, type **192.168.2.1** and log in using the user name and password you previously configured in order to access the configuration pages.
2. Click the **Firewall** tab.
3. Scroll down to the **Port Triggering** section.
4. Select **TCP** for the **Outbound protocol**.

Outbound protocol: 

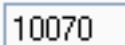
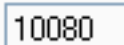
5. For **Outbound port range**, enter **10070** in the first box, and **10080** in the second box.

Outbound port range:  to 

6. Select **TCP** for the **Inbound protocol**.

Inbound protocol: 

7. For **Inbound port range**, enter **10070** in the first box, and **10080** in the second box.

Inbound port range:  to 

8. For **Destination port range**, enter **10070** in the first box, and **10080** in the second box.

Destination port range: to

9. Click **Add**.

Add

On the page, you should see the rules for TCP ports 10070 to 10080.

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☒	TCP	10070 to 10080	TCP	10070 to 10080	10070 to 10080	Delete

10. Next, select **UDP** for the **Outbound protocol**.

Outbound protocol:

11. For **Outbound port range**, enter 10070 in both boxes.

Outbound port range: to

12. Select **UDP** for the **Inbound protocol**.

Inbound protocol:

13. For **Inbound port range**, enter 10070 in both boxes.

Inbound port range: to

14. For **Destination port range**, enter 10070 in both boxes.

Destination port range: to

15. Click **Add**.

Add

On the page, you should see the rule for UDP port 10070.

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☒	TCP	10070 to 10080	TCP	10070 to 10080	10070 to 10080	Delete
☒	UDP	10070 to 10070	UDP	10070 to 10070	10070 to 10070	Delete

16. Click **Save** at the bottom of the page when you are finished.

[Return to Tutorials page](#)





© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

Regulatory Information

Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC's specifications:

Part 15, Class B

Operation of this device is subject to the following conditions:

- 1) this device may not cause harmful electromagnetic interference, and
- 2) this device must accept any interference received including interference that may cause undesired operations.

This equipment complies with FCC Part 15 for Home and Office use.

Caution to the User: Any changes or modifications not expressly approved by the party

responsible for compliance could void the user's authority to operate the equipment.

Detachable Antenna Information

FCC Part 15, Subpart C, Section 15.203 Antenna requirement

5464 users: An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device. The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply with the provisions of this section. The manufacturer may design the unit so that a broken antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Radio and Television Interference:

This equipment has been tested and found to comply with the limits for a Class B digital device, 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. If this equipment is not installed and used in accordance with the manufacturer's instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to 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.

USR declares 5464 is limited in CH1~11 from 2412 to 2462 MHz by specified firmware controlled in USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

UL Listing/CUL Listing:

This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide. Use this product only with UL Listed Information Technology Equipment (ITE).

For Canadian Users

Industry Canada (IC)

This equipment complies with the Industry Canada Spectrum Management and Telecommunications policy, RSS-210, standard Low Power License-Exempt Radio Communication Devices.

Operation is subject to the following two conditions:

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.

Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropic Radiated Power (EIRP) is not more than that required for successful communication.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



CE Compliance

Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157 USA, declare under our sole responsibility that the product, USRobotics Wireless *Nd₁* Router, Model 5464, to which this declaration relates, is in conformity with the following standards and/or other normative documents.

EN300 328
EN301 489-1
EN301 489-17
EN60950-1
EN61000-3-2
EN61000-3-3
EN50392

We, U.S. Robotics Corporation, hereby declare the above named product is in compliance and conformity with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The conformity assessment procedure referred to in Article 10 and detailed in Annex IV of Directive 1999/5/EC has been followed.

This equipment is in compliance with the European recommendation 1999/519/ECC, governing the exposure to the electromagnetic radiation.

This product can be used in the following countries: Germany, Austria, Belgium, Switzerland, Netherlands, Luxembourg, Italy, France, UK, Ireland, Spain, Portugal, Sweden, Norway, Denmark, Finland, Czech Republic, Poland, Hungary, and Greece.

An electronic copy of the original CE Declaration of Conformity is available at the U.S. Robotics website: www.usr.com.

Regarding IEEE 802.11b/g frequencies, we currently have the following information about restrictions in the European Union (EU) countries:

- Italy

Please be aware that use of the wireless device is subject to the following Italian regulation:

1. D.Lgs 1.8.2003, number 259, articles 104 (activities where General Authorization is required) and 105 (free use), for private use;
2. D.M 28.5.03 and later modifications, for the supplying to public RadioLAN access for networks and telecommunication services

- France

In France metropolitan, outdoor power is limited to 10mW (EIRP) within 2454MHz – 2483, 5MHz frequency band

In Guyana and Reunion Islands, outdoor use is forbidden within 2400MHz – 2420MHz frequency band

Regulatory Channel Frequency

Channel	Frequency (MHz)	FCC	Canada	ETSI
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467			X
13	2472			X

Operating Channels:

- IEEE 802.11g compliant
- 11 channels (US, Canada)
- 13 channels (ETSI)

EU Health Protection

This device complies with the European requirements governing exposure to electromagnetic radiation. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This wireless device is a transmitter/receiver and has been designed and manufactured to comply with the exposure limits recommended by the Council of the European Union and the International Commission on Non-Ionizing Radiation Protection (ICNIRP, 1999) for the entire population. The exposure standard for portable equipment uses the "Specific Absorption Rate" as unit of measure. The maximum SAR value of this wireless device measured in the conformity test is **X.XX** W/Kg.

EU Detachable Antenna Information

This USRobotics wireless device has been designed to operate with the antenna included in this package only. Together this device and antenna combination has been tested and approved by a European Agency conforming with the European R&TTE directive 1999/5/EC to meet the radiated power level requirement of 100mW (EIRP). Replacement of this antenna must only be done with an authorized USRobotics component that has been designed and tested with the unit to the requirements of directive 1999/5/EC. Please refer to the U.S. Robotics Web site to get product antenna ordering information.

Go to www.usr.com to see the most recent channel restriction information.





- **Home**
- **Installation**
- **Configuration**
 - **Tutorials**
 - **Help**

Copyright Information

U.S. Robotics Corporation
935 National Parkway
Schaumburg, Illinois
60173-5157
USA

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as a translation, transformation, or adaptation) without written permission from U.S. Robotics Corporation. U.S. Robotics Corporation reserves the right to revise this documentation and to make changes in the products and/or content of this document from time to time without obligation to provide notification of such revision or change. U.S. Robotics Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact U.S. Robotics and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in U.S. Robotics standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987) whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this Quick Installation Guide.

Copyright © 2006 U.S. Robotics Corporation. All rights reserved. U.S. Robotics and the U.S. Robotics logo are registered trademarks of U.S. Robotics Corporation. Other product names are for identification purposes only and may be trademarks of their respective companies. Product specifications subject to change without notice.



© 2006 U.S. Robotics Corporation



- Home
- Installation
- Configuration
 - Tutorials
 - Help

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U.S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U.S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage caused by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A.

excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A



© 2006 U.S. Robotics Corporation