Network Test (Ping)

You can use this to see if the router can reach a server on the Internet or a device on your network. Enter a valid IP address or domain name and click the **Ping** button.

IP address: www.usr.com [Ping]

You can test your network connection directly from the router configuration pages by entering an **IP address** or domain name and clicking the **Ping** button.

The router will attempt to contact the device at the IP address, and will respond, telling you if the attempt failed or responded. To go back to the **Status** page, click **Continue**.

© 2006 U.S. Robotics Corporation

USRobotics *Wireless Nd1 Router User Guide*

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

Log Information

This log displays TCP/UDP LAN and WAN interface traffic which is destined for the router. This can help you detect if any unauthorised users are attempting to access your network.

The **Refresh** button will update the log to show the most recent information. If you have host set in your **System Log** settings, the router log will be sent to the System Log host when you click **Refresh**.

USRobotics *Log*

Status | Log | Internet | Security | Firewall | Wireless | LAN | Device

Refresh

TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1143
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1144
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1145
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1146
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1148
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1147
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1149
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1150
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1151
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1152
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1153
TCP connection accepted to 192.168.2.1:80 from 192.168.2.2:1154
TCP ... 192.168.2.2:1155

Router Log

In the Router Log area, you can specify which activities will be logged.

Router Log

Log accepted and denied connections

No log
Log denied connections only
Log accepted connections only
Log accepted and denied connections

The system log transmits its entries to a client device on the network.

- If you select **No log**, no log information will be recorded.

- If you select **Log denied connections only**, any unsuccessful attempts, by a client, to connect to your router will be recorded.

- If you select **Log accepted connections only**, any successful attempts, by a client, to connect to your router will be recorded.

- If you select **Log accepted and denied connections**, any successful or unsuccessful attempts, by a client, to connect to your router will be recorded.

System Log

System Log

The system log transmits its entries to a client device on the network.

☐ System log

Using this feature you can configure the router to send its system log to a remote host. The system log is sent using User Datagram Protocol (UDP) with destination port 514 by default.

1. Select the checkbox next to **System log** in the System Log section.

> **Note**: The router can only send system logs to hosts reachable on its LAN interface.

2. Specify the **IP address** of the remote host and remote port (if applicable).

Example: **192.168.2.10:520** sends the log to the host with IP address 192.168.2.10 at port 520.

3. Click **Save** after you have completed all your changes on this page to apply the new settings to the router.

© 2006 U.S. Robotics Corporation

USRobotics *Wireless Nd1 Router User Guide*

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

Internet Connection Settings

1. Select your Internet connection type and then enter the appropriate information for the connection:

   - Cable, DSL Router, satellite, ISDN, LAN, or other

   - DSL modem (also known as PPPoE)

   > **Note**: If you do not know what type of Internet connection you have, contact your Internet Service Provider.

2. If your ISP uses Point-to-Point Tunneling (PPTP), after you have configured your Internet Connection in Step 1, select **My ISP uses a PPTP connection** and enter the Domain or IP address of your PPTP server in the **Server** field, and the **User name** and **Password** from your ISP. If your ISP uses a specific authentication method, either select or deselect the appropriate checkboxes.

Point-To-Point Tunneling (PPTP)

If your ISP provided you with information about using the Point-to-Point Tunneling Protocol (PPTP) to establish a Virtual Private Network (VPN) to connect to the Internet, enter it here. (This is not common.)

☑ My ISP uses a PPTP connection.

Server: _____
(Enter a domain—such as "myisp.com"—or an IP address.)

User name: _____

Password: _____

Please select the supported authentication methods. If you're not sure, you can keep the defaults.

☑ CHAP
☑ MSCHAP
☑ MSCHAP-V2
☐ PAP (not common)

MTU: 1460 bytes

MRU: 1460 bytes

3. If your ISP requires you to use a host name, enter it in **Host Name**.

Host Name

If your ISP provided you with a host name, enter it here.

Host name: _____

4. If your ISP requires a specific MAC address for the Internet connection, you will need to change the MAC address of the router. Either select the MAC address from the **Client devices** list or enter it manually in the **Router** field.

5. Remote Access allows any host on the entire WAN network to connect to the router's configuration pages. By default, only devices that are connected to the router via an Ethernet cable at a LAN port can access the router's configuration pages. To enable Remote Access, select **Allow access to this router from the Internet**. By default, the port "8080" is assigned. If you wish to use another port, enter the port number.

6. To enable remote access to the printer attached to the router from outside the LAN, select **Allow access to the print server from the Internet**.

Note: You need to click **Save** to save all your new settings and reboot the router after you have completed all your changes.

Static Routes

Static Routes

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

IP address: _____

Subnet mask: _____

Gateway: _____

Hops: _____

[Add]

If you make a physical connection from the router's WAN port to an existing network or networks, you may need to establish Static Routes. This will allow the router to use its own network address, which is different from the network to which it is connected. This will also allow the router to connect to specific networks that already exist on the WAN side.

For Static Routes on your WAN, you must use values within the same subnets as your Internet connection.

Note: The default LAN IP address of the router is **192.168.2.1** and default Subnet Mask is **255.255.255.0**.

1. Enter the IP address of the network for this specific router in the **IP address** field.

2. Enter the Subnet mask of the network for this specific router in the **Subnet mask** field.

3. Enter the Gateway of the network for this specific router in the **Gateway** field.

4. Enter the number of routers that this router must connect through in order to connect to the other network in the **Hops** field.

   The number of hops is determined by how many routers are between your router and the respective network.

   Example: If there is another router connected to the router 's WAN port, you would enter **1** for the number of hops between the router's WAN port and any client connected to the second router.

5. Click **Add**.

Dynamic DNS

A DNS (Domain Name Service) resolves an Internet address such as **www.usr.com** into an IP address. A dynamic DNS service allows you to assign a Web name like **myUSRrouter.dynDNS.com** to your gateway, making it accessible from the Internet without having to know the gateway's IP address assigned by the service provider.

In this page, you can set parameters that will allow the domain name services to find your gateway. You would use this to bypass the dynamic nature of WAN IP addressing, to have a consistent host name accessible from the Internet.

Note: You will need dynamic DNS service provided by a third party to use this feature.

To configure Dynamic DNS on your router:

1. Select your DNS provider. You can register at **DynDNS.org**, **TZO.com**, **DtDNS.com**, and **No-IP. com** for no charge.

2. Enter your dynamic DNS settings, including **Host name**, **User name** and **Password**, given to you by the DNS provider. Click **Add** when you're done.

To remove a dynamic DNS assignment, click the **Delete** button next to the DNS assignment.

Note: You need to click **Save** to save all your new settings and reboot the router after you have completed all your changes.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Cable, DSL Router, satellite, ISDN, LAN, or other

> **Note**: If your Internet connection uses a static IP address, you may need to contact your Internet Service Provider for the following information: **IP Address**, **Subnet Mask**, **Gateway**, **DNS Servers**, and **WINS Servers**

If the router uses DHCP, your Internet connection should have been automatically detected. If the router could not detect the connection, see Troubleshooting.

If your ISP requires you to use a static IP address, check **My ISP provided an IP address for my Internet connection** and enter the **IP address**, **Subnet mask**, **Gateway**, and **DNS servers** information from your ISP.

Static IP Address

☑ My ISP provided an IP address for my Internet connection (such as "210.123.1.54").

Static IP address: `0.0.0.0`

Subnet mask: `0.0.0.0`

Gateway: `0.0.0.0`

DNS servers:

WINS servers:

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

DSL modem (also known as PPPoE)

> **Note**: If your Internet connection uses PPPoE, you may need to contact your Internet Service Provider for the following information: **User Name**, **Password** and **Service Name**

1. Enter the **User name** and **Password** information, if required by your ISP:

Internet Login (PPPoE)

If your ISP provided a user name and password for your Internet connection, please enter them here.

This is also known as a PPPoE connection. You should not enter your user name and password if you have PPPoA or if you have a DSL router (or another device, such as a VoIP gateway) that you've already configured with your user name and password.

User name: [   ]
Password: [   ]

2. Enter the connection information, as required by your ISP:

Internet Connection (PPPoE)

☐ Disconnect if inactive for [1   ] minutes

Service name: [   ]
MRU: [1492   ] bytes
MTU: [1492   ] bytes

- ○ **Disconnect if inactive for**: Specify a timeout for your Internet connection to be disconnected if your Internet connection is not active.
- ○ **Service name**: The PPPoE Service Name is an ISP name or a class of service that is

configured on the PPPoE server.

 ❍ **MRU**: The MRU is the largest packet size the router will allow a computer on the network to receive. MRU stands for Maximum Receive Unit. Contact your ISP if you have any questions regarding what this number should be or if it is necessary. If your ISP does not instruct you to change this number, leave the default setting of 1492.

 ❍ **MTU**: The MTU is the largest packet size the router will allow a computer on the network to send. MTU stands for Maximum Transmission Unit. Contact your ISP if you have any questions regarding what this number should be or if it is necessary. If your ISP does not instruct you to change this number, leave the default setting of 1492.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Security Settings

The **Security** page lets you configure and change the security settings for the router, including your wireless security settings, MAC address filtering options, and login information.

Router Login

Router Login

You will need to enter the user name and password in order to access the router in the future, so you may want to write them down.

User name: admin
Password: password

This displays the current user name and password assigned to the router. 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 **N**d_1 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.

Wireless

In this section you can enable the wireless security features. USRobotics strongly recommends that you enable some form of wireless security so that unauthorised clients are not able to access your network. All the wireless devices you want to connect to the network must have the same security settings including the pass phrase or key that you use to secure your wireless network.

> **Note**: For your wireless security settings, it is recommended that you select the **WPA2 and WPA (PSK)** or **WPA2 and WPA with 802.1x (RADIUS)** wireless security method using **TKIP and AES** encryption for the most secure wireless network.

Select the encryption **Method** that you want the wireless network to use. You can select from the following methods and enter the pass phrase or key:

- **WPA2 and WPA (PSK):** You need to set your **Encryption** type to **TKIP and AES**, **AES,** or **TKIP**. You will then need to enter a **Pass phrase** (which is also commonly called a *Network key*, *WPA key*, or *WPA Pre-shared key*). The pass phrase must be between eight and sixty-three characters in length. This pass phrase must be the same on each computer that is connected to the wireless network. You can also specify a **Key rotation**, in seconds, or enter **0** in the field to disable the option.

- **WPA2 (PSK):** You need to set your **Encryption** type to **AES** or **TKIP**. You will then need to enter a **Pass phrase** (which is also commonly called a *Network key*, *WPA key*, or *WPA Pre-shared key*). The pass phrase must be between eight and sixty-three characters in length. This pass phrase must be the same on each computer that is connected to the wireless network.

- **WPA (PSK):** You need to set your **Encryption** type to **TKIP and AES, AES,** or **TKIP**. You will then need to enter a **Pass phrase** (which is also commonly called a *Network key*, *WPA key*, or *WPA Pre-shared key*). The pass phrase must be between eight and sixty-three characters in length. This pass phrase must be the same on each computer that is connected to the wireless network.

> **Note**: Not all wireless clients support AES encryption when using WPA (PSK) security. TKIP encryption with WPA (PSK) is supported by most wireless clients. You can assign the router WPA (PSK) security with the **TKIP and AES** encryption to cover both AES and TKIP clients.

- **WEP open:** You need to set your **Key type** to **128-bit ASCII, 128-bit hex, 64-bit ASCII** or **64-bit hex**. Then, enter the **Key** (which is also commonly called a *Network key*). The Key must be 13 characters long for a 128-bit ASCII key type, 26 characters long for a 128-bit hex key type, and 5 characters long for a 64-bit ASCII key type or 10 characters long for a 64-bit hex key type.

- **WEP shared:** You need to set your **Key type** to **128-bit ASCII, 128-bit hex, 64-bit ASCII** or **64-bit hex**. Then, enter the **Key** (which is also commonly called a *Network key*). The Key must be 13 characters long for a 128-bit ASCII key type, 26 characters long for a 128-bit hex key type, and 5 characters long for a 64-bit ASCII key type or 10 characters long for a 64-bit hex key type.

- **WPA2 and WPA with 802.1x (RADIUS)**: You need to set your **Encryption** type to **TKIP and AES**, **AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.

- **WPA2 with 802.1x (RADIUS)**: You need to set your **Encryption** type to **TKIP and AES**, **AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.

- **WPA with 802.1x (RADIUS)**: You need to set your **Encryption** type to **AES** or **TKIP**. Then you need to enter the **RADIUS server** IP address and **RADIUS Port**. You will then need to enter the **RADIUS key**.

> **Note**: Not all wireless clients support AES encryption when using WPA (PSK) security. TKIP encryption with WPA is supported by most wireless clients.

- **None**: This disables all wireless security on your router.

> **Note:** The setting of **None** is not recommended since without any encryption enabled, your network will be vulnerable to outside malicious attacks

MAC Filter

In this area you can control which wireless devices are allowed or denied access to the router based upon their MAC addresses. The MAC address can usually be found either on a label on the external wireless product or in the configuration utility of the wireless client, depending on the wireless device you are using.

MAC Filter

Use this section to allow (or deny) specific wireless devices the ability to connect to the router. For example, you could specify that only your laptop, gaming system and digital video recorder can connect. (Please note that wired clients are always permitted to connect.)

| **Allow Current Clients** | Press the **Allow Current Clients** button to automatically permit the current wireless client devices to connect to the router. (The changes aren't saved until you press the **Save** button.) |

Filter: Allow all wireless devices

The router configuration pages let you configure access to the router based on MAC addresses by using the **Allow Current Clients** button or specify a level of filter to apply:

- Click **Allow Current Clients** to allow all of the wireless clients currently connected to the router to be allowed access to the router in the future. By default, the filter setting of **Allow only these devices** will then be applied.

- **Allow all devices**: Any wireless client that has the correct security information will be allowed to connect to the router. *This is the default setting.*

- **Allow only these devices**: Allows only devices with specific MAC addresses to establish a wireless connection with the router.

    1. Enter the MAC address of the device that should be allowed connection to the

router.

2. Click **Add**.

- **Deny only these devices**: Denies a wireless connection to the router for devices with the specified MAC addresses. This can be used if you notice unauthorised wireless devices that are connected to your network.

  1. Enter the MAC address of the device that should be denied connection to the router.

  2. Click **Add.**

Note: You need to click **Save** to save all your new settings and reboot the router after you have completed all your changes.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Firewall Settings

The firewall built into the router protects your network from outside attacks, and controls access to the Internet from your network. In the configuration pages, select **Firewall**. In this section you can configure and change the Firewall settings for the router.

Internet Access Control

With this option, you can deny Internet access to specific clients during specific days and times of the week. This can be useful if you have children in your home and you want to regulate their Internet usage or if you have multiple people in your small business using the same computer over different shifts and you don't want specific employees to be able to access the Internet.

The router comes with two default access control rules to restrict Internet access to computers with IP addresses between the range of 192.168.2.100 and 192.168.2.110. To enable a 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.

For detailed steps on configuring your own Internet Access Control rules, see the Parental Controls section on the Tutorials page.

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 ▼]

[Add]

To add entries for this feature, you will need to complete the following steps:

1. Specify the range of **LAN IP addresses** or a single IP address.

2. Specify the **Protocol**, either **TCP** (Transmission Control Protocol) or **UDP** (User Datagram Protocol).

3. Specify the **Port range** or enter a single specific port to block.

4. Specify the **Weekday range** and the **Time range each day**.

5. When you have specified these settings, click **Add**.

6. Repeat steps 1 through 4 for any additional entries.

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

Port Triggering

Some applications connect to the Internet by using one or more outbound ports expecting the remote host to connect back at one or more inbound ports. The router, by default, blocks all incoming connections. Port Triggering configures the router's firewall to allow the incoming connections to reach the client devices.

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.

For detailed steps on configuring your own Port Triggering rules, including Port Triggering details for a Microsoft Xbox®, see the Tutorials page.

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.

For a complete list of applications and port information, visit www.iana.org

Port Triggering

On	Outbound Protocol	Ports	Inbound Protocol	Ports	Destination Ports	
☐	TCP	1 to 65535	TCP	10070 to 10080	10070 to 10080	Delete
☐	UDP	1 to 65535	UDP	10070 to 10070	10070 to 10070	Delete

Outbound protocol: [TCP ▾]

Outbound port range: [   ] to [   ]

Inbound protocol: [TCP ▾]

Inbound port range: [   ] to [   ]

Destination port range: [   ] to [   ]

[Add]

To add entries for this feature, complete the following steps:

1. Specify the **Outbound protocol** (TCP/UDP).

2. Specify the **Outbound port range** of the destination ports for outbound traffic which will cause this Port Trigger to activate.

3. Specify the **Inbound protoco**l (TCP/UDP).

4. Specify the **Inbound port range** of the destination ports for inbound traffic. The router will allow inbound traffic on these ports when the Port Trigger is active.

5. Specify the **Destination port range** for the ports the inbound connection will be translated to. When this Port Trigger is active, the router will translate the destination

port of an inbound connection to this port range.

6. When you have specified these settings, click **Add**.

7. Repeat steps 1 through 5 for any additional entries.

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

Port Forwarding

With **Port Forwarding**, you can direct inbound traffic to specific clients on your network. Ports are connections that are used by a computer to organize the various forms of network traffic. A port can support both ingoing and outgoing network traffic, or just one-way network traffic.

If you open a port, a specific service will be assigned to it and that service will communicate with the network only through that port. Some applications require open service ports, such as Internet games, video conferencing, Internet telephony, and others.

An example of when you might want to enable this feature is if you are running a Web server on one of your network clients. By enabling Port Forwarding, traffic to that Web site would pass through the router and go directly to the appropriate network client, instead of going through the router and suddenly having access to your whole network.

As an example, the router comes with a default port forwarding rule for a Web server on your network where the ports for Web traffic (80) need to direct to the IP address for the Web sever (default IP address: 192.168.2.120). To enable the rule, select the **On** checkbox for the rule.

For detailed steps on configuring your own Port Forwarding rules, see the Tutorials page.

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.

Port Forwarding

On	Protocol	WAN Ports	LAN IP Address	LAN Ports	
☐	TCP	80 to 80	192.168.2.120	80 to 80	Delete

Protocol: TCP

WAN port range: ___ to ___

LAN IP address: ___
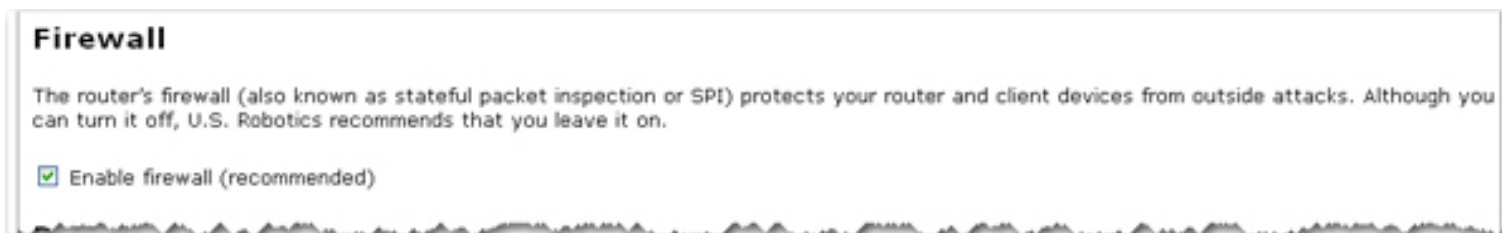
LAN port range: ___ to ___

Add

To add entries for this feature, complete the following steps:

1. Specify the **Protocol** and the **WAN port range**. The router will allow incoming traffic on these incoming ports of the previously mentioned protocol type to pass through the firewall.

2. Specify the **LAN IP address** and the **LAN port range** of ports the incoming traffic will be forwarded to.

3. When you have specified these settings, click **Add**.

4. Repeat steps 1 through 3 for any additional entries.

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

Firewall

If you deselect the checkbox next to **Enable firewall**, the firewall will be disabled, but this is not recommended. The firewall is used to block unauthorised users from accessing the network or any of the network resources. A firewall is one of the most critical pieces of security you can use in your network.

Firewall

The router's firewall (also known as stateful packet inspection or SPI) protects your router and client devices from outside attacks. Although you can turn it off, U.S. Robotics recommends that you leave it on.

☑ Enable firewall (recommended)

DMZ

The DMZ (Demilitarised Zone) is a computer that has all external Internet traffic forwarded to it, such as a public Web server. This allows a computer to be exposed to unrestricted two-way communication. This feature should be used with caution, since it removes the security of the firewall for that computer.

DMZ

The DMZ is a client device that is outside—and not protected by—the router's firewall. If you host a public web server on a computer on your network, you might specify its IP address here.

IP address: [   ]

If you want to specify a DMZ, enter the client computer's **IP address**. When you are finished, click **Save**.

Note: You need to click **Save** to save all your new settings and reboot the router after you have completed all your changes.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Wireless Settings

Note: If you used SecureEasySetup to configure your wireless security settings, changing the **Network Name** or other security settings for your router will cause your connected wireless clients to loose connectivity with the router.

In this section you can enable the wireless security features. USRobotics strongly recommends that you enable some form of wireless security so that unauthorised clients are not able to access your network.

Note: All the wireless devices you want to connect to the network must have the same wireless security settings including the pass phrase or key that you use to secure your wireless network.

To enable the wireless functions on your router, verify that **Allow wireless connections** is checked.
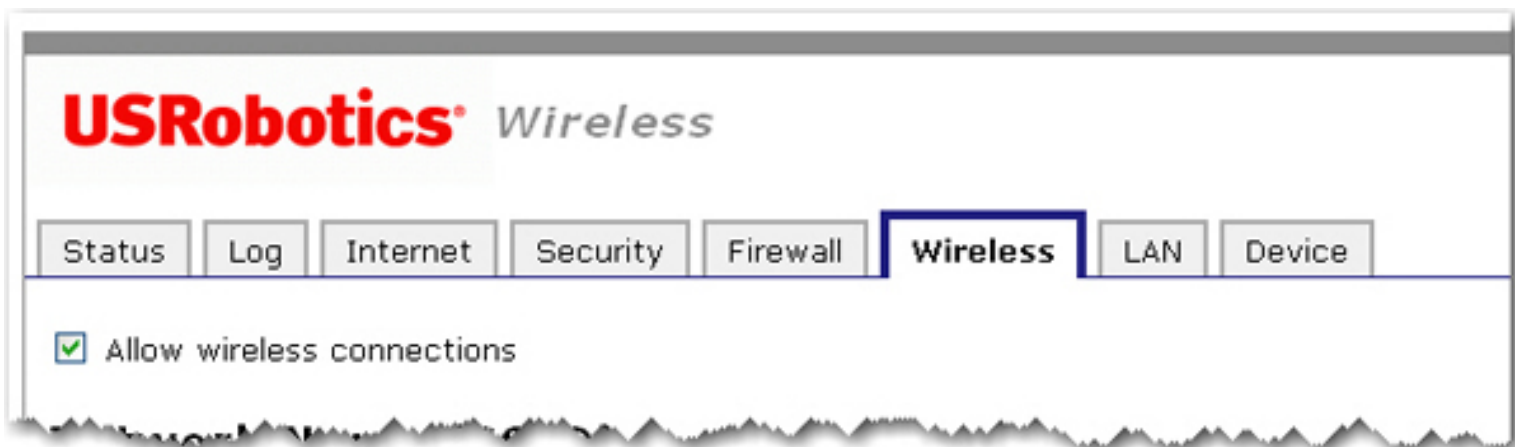
Network Name (SSID)

Wireless clients use the **Network name** (SSID) to connect to your router.

The default **Network name** of the router is USR5464. If you want to use multiple Wireless **N**d_1 routers independently, you must configure a unique Network name for each router.

> **Note**: If you are using multiple Wireless **N**d_1 routers and you want them to use independently, each router will need a unique Network name.

Select **Broadcast network name** if you want wireless devices to be able to detect your router when they perform a site scan.

If you deselect **Broadcast network name**, wireless devices will not be able to detect your wireless network during a site scan. Devices will have to manually enter the Network Name (SSID) of your router to connect.

Access Point Isolation

If the router will be used in a public place where you do not want any wireless clients to be able to share files or printers between themselves, select **Access point isolation**. With this selected, all of the wireless clients will only be able to access the Internet. An example of a situation where you would want to enable this feature is in a public hotspot, such as a coffee shop or hotel. This feature is disabled by default.

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.

By default, this mode is turned off and the router is in **Access Point** mode where it accepts

wireless connections.

If you enable Bridge mode and WDS Restrictions in the wireless router, a bridge will be created to another wireless router or access point and no wireless clients will be able to connect to the wireless network. This is generally used when you want to connect two networks that are in different buildings. Each wireless router or access point will have to have the MAC address of the other device entered in the WDS Restrictions table.

With Bridge mode, you will only be able to use the following forms of encryption methods: **WPA (PSK)**, **WEP open**, **WEP shared**, or **None**. For your encryption type, you can choose either **TKIP** or **AES**, but not **TKIP and AES**.

Note: In Bridge mode, the Wireless **N**d_1 Router does not support Wi-Fi Multimedia (WMM).

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

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

WDS Restrictions

USRobotics routers and Access Points are capable of using a feature known as WDS (Wireless Distribution System) which allows the wireless router or access point to connect directly to another wireless router or access point, while still allowing wireless clients to connect to the network.

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

If you select **Enable WDS restrictions**, you will need to 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.
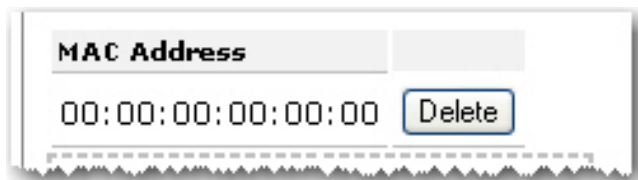
You can find information about this advanced feature in the user manual on the installation CD-ROM.

☑ Enable WDS restrictions

MAC address:

[   ] [Add]

To delete an existing WDS mapping, click the **Delete** button next to the MAC Address.

WDS allows you to use multiple access points or wireless routers to connect several separate networks together. By connecting an access point or wireless router to each network and enabling the WDS feature, the wireless clients in the immediate area will be able to connect to the wireless network while a bridge would also be created to another access point or wireless router that is further away. The wireless router and the wireless product that you will be creating a bridge with will need to have the same channel selected, the same **Network Name** (SSID), same wireless security settings, as well as the MAC address of the other device entered in the WDS Restrictions table. Enabling the WDS Restrictions option allows you to enter the MAC addresses of the access points or wireless routers that will be capable of connecting to each point of the wireless network that you have created. This will then limit exactly who has access to the wireless network.

One thing to note about this type of wireless network is that the throughput may be reduced for the bridging portion. Therefore, bridged routers or access points that also allow wireless clients to connect to the network should not be used for high-volume traffic. Some examples of the type of situations where you might want this type of network would be for security cameras, to provide network access to certain parts of a building that might not be able to be connected using wires, or to provide short-term network access to a conference area.

If you enable Bridge mode and WDS Restrictions in the wireless router, a bridge will be created to another wireless router or access point and no wireless clients will be able to connect to the wireless network. This is generally used when you want to connect two networks that are in different buildings. Each wireless router or access point will have to have the MAC address of the other device entered in the WDS Restrictions table.

The router's WDS connections do not support: **WPA2 (PSK)** or any of the **RADIUS** security methods, nor **TKIP and AES** encryption.

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)** with **TKIP and AES**

- **WPA2 (PSK)** with **TKIP**

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

- **WPA (PSK)** with **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)** with **AES**:

- **WPA2 (PSK)** with **AES**

- **WPA (PSK)** with **AES**

In both of these cases, 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.

Wi-Fi Multimedia (WMM)

This feature is disabled by default. If you want to enable this feature, select the checkbox next to **Enable WMM** (Wi-Fi Multimedia). The other devices that you are connecting to in order to use this feature must also support WMM and have it enabled.

This feature enables the Quality of Service (QoS) function that is used for multimedia applications, such as Voice-over-IP (VoIP) and video. This allows the network packets of the multimedia application to have priority over regular data network packets, allowing multimedia applications to run smoother and with fewer errors.

Wi-Fi Multimedia (WMM)

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

☐ Enable WMM

If you enable WMM, you can then select **Enable no-acknowledgement**. No-Acknowledgement refers to the acknowledge policy used at the MAC level. Enabling no-acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.

Wi-Fi Multimedia (WMM)

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

☑ Enable WMM

☑ Enable no-acknowledgement

☑ Enable APSD (Automatic Power Save Delivery)

With WMM enabled, you can also select **Enable APSD (Automatic Power Save Delivery)**. APSD manages radio usage for battery-powered devices to allow longer battery life in certain conditions. APSD allows a longer beacon interval until an application requiring a short packet exchange interval starts. Voice Over Internet Protocol (VoIP) is an example of application requiring a short packet exchange interval. APSD affects radio usage and battery life only if the wireless client also supports APSD.

Transmission

The fields in this area are for more advanced wireless features that most people do not need to change. If you do want to change any of these settings, write down the default settings before you make any changes in case you experience any problems and need to change these settings back.

Control and Extension Channels

Control and the secondary extension channels are only applicable if your router is operating at 40 MHz bandwidth and the **802.11n mode** is configured as **Automatic**.

For US channels:

Control Channel	Sideband	Extension Channel
1 - 7	Lower	Channel number + 4
5 - 11	Upper	Channel number - 4

For European channels:

Control Channel	Sideband	Extension Channel
1 - 9	Lower	Channel number + 4
5 - 13	Upper	Channel number - 4

Example: If your control channel is set to 1, the extension channel will be transmitted on channel 5. The total bandwidth of the signals on channel 1 and 5 equals 40 MHz.

Example: If your control channel is set to 11, the extension channel will be transmitted on channel 6. The total bandwidth of the signals on channel 11 and 7 equals 40 MHz.

Transmission

These are advanced settings and most people won't need to modify them. You can find information about these advanced features in the user manual on the installation CD-ROM.

Power level: `100% ▾`

Control channel: `11 ▾`

802.11n mode: `Automatic ▾`

Bandwidth: `20 MHz ▾`

Sideband for control channel: `Lower ▾`

NPHY rate: `Automatic ▾`

☑ Automatic 802.11n protection

Multicast rate: `Automatic ▾`

Basic rate set: `Default ▾`

Acceleration: `54g+ (XPress™) ▾`

☐ Enable VLAN priority mode

Beacon interval: `100` ms (recommended to be between 1 and 1000 ms)

RTS threshold: `2347` (must be between 256 and 2347)

Fragmentation threshold: `2346` (must be between 256 and 2346, even numbers only)

DTIM interval: `1` (must be between 1 and 255)

Preamble: `Long ▾`

When you fini...

- **Power level**: Select either 100%, 50%, or 25% from the drop-down menu. The Power level sets the strength of the wireless signal that the router transmits. You would want a lower setting if you live in an area where your wireless signal could be overlapping with other wireless networks and want to reduce the interference you encounter.

- **Control Channel**: Sets the channel on which the router operates. If you are experiencing interference or wireless network problems, changing the channel may solve the issue. It is recommended that you keep the control channel set at "Automatic" to avoid interference with adjacent networks.

- **802.11n mode**: You can select **Automatic**, or **Off**. **Automatic** enables 802.11n support, and **Off** will disable 802.11n support.

- **Bandwidth**: Specify radio frequency bandwidth, either **20MHz** or **40MHz** (dual channel), that the router will use if **802.11n mode** is configured as **Automatic**. If the router detects other adjacent wireless networks, it will use 20 MHz operation so as to not interfere with the networks. If there no other adjacent networks are detected, the

router will use 40MHz operation.

In both 20 MHz and 40 MHz operation, when the **802.11n mode** is configured to **Automatic**, the router will use dynamic channel selection to determine the best channels to transmit in order for optimal operation.

- **NPHY rate**: Set the Physical Layer (NPHY) rate. These rates are only applicable when the **802.11n mode** is configured as **Automatic**.

- **Automatic 802.11n protection**: If you select this option, the router will use Request to Send/Clear to Send (RTS/CTS) to improve the performance in 802.11 mixed environments. If this is not selected, the 802.11 performance will be maximized under most conditions while the other 802.11 modes (802.11b, etc.) will be secondary.

- **Legacy rate**: Set the Physical Layer rate. This option is only visible when **802.11n mode** is turned **Off**.

- **Multicast rate**: Specify the rate at which multicast packets are transmitted and received on your wireless network. Multicast packets are used to send a single message to a set of recipients in a defined group. Teleconferencing, videoconferencing and group email are some examples of multicast applications. Specifying a high multicast rate may improve performance of multicast features. The rates are in Mbps. You can select **Automatic**, **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, **54**.

- **Basic rate set**: Select the basic rate that wireless clients must support, either **Default**, **All**, or **1 & 2 Mbps**.

- **Acceleration**: Select **None**, or **54g+ (Xpress™)**. These features determine either normal speed rates or accelerated rates. Set the mode to **54g+ (Xpress™)** for the widest compatibility. Set the mode to **None** if you are experiencing difficulty with legacy 802.11b/g equipment.

- **Enable VLAN priority mode**: When selected, the router will advertise packet priority using the VLAN tag.

- **Beacon Interval:** The amount of time between beacon transmissions. A beacon is basically a heartbeat for a wireless client or router, sending out a signal informing the network that it is still active. This should be set between 1 and 1000 milliseconds. The default beacon interval is 100 ms.

- **RTS threshold**: The RTS Threshold is the minimum size in bytes for which the

Request to Send/Clear to Send (RTS/CTS) channel contention mechanism is used. In a network with significant radio interference or large number of wireless devices on the same channel, reducing the RTS Threshold might help in reducing frame loss. The RTS threshold is 2347 bytes by default, which is the maximum value.

- **Fragmentation threshold**: The maximum level the router will reach when sending information in packets before the packets are broken up in fragments. Typically, if you are experiencing problems sending information, it is because there is other traffic on the network and the data being transmitted is colliding. This might be corrected by the information being broken into fragments. The lower the level that the Fragmentation threshold is set to, the smaller a packet has to be before it is broken into fragments. If the maximum is set (2346), fragmentation is essentially disabled. You should only change this level if you are an advanced user.

- **DTIM Interval**: This parameter configures the amount of time after which buffered broadcast and multicast frames will be delivered to the wireless clients. This allows mobile stations to conserve power. If you are using applications which use broadcast or multicast frames for delivering data, you should use a Delivery Traffic Indication Message (DTIM) Interval of 1 to minimize delay for real-time traffic, such as multicast audio and video streams.

- **Preamble**: Defines the length of the Cyclic Redundancy Check (CRC) block for communication between the router and wireless clients. The preamble consists of the Synchronization and Start Frame Delimiter (SFD) fields. The sync field is used to indicate the delivery of a frame to wireless stations, to measure frequency of the radio signal, to perform corrections if needed. The SFD at the end of the Preamble is used to mark the start of the frame.

  If you are not using any 802.11b devices in your network, you can configure the Preamble type to **Short** for optimum performance. The **Long** Preamble type should be used when both 802.11g and 802.11b devices exist on your network.

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

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Local Area Network (LAN) Settings

From the **LAN** page, you can view and modify the Local Area Network (LAN) settings of the router. These settings apply only to your local network.

IP Address

Your router automatically has its IP address and Subnet Mask configured. If you need change these values, enter your new **IP Address** and **Subnet mask** and click **Save** at the bottom of the page.

When you change the IP address of your router, you may need to release and renew the IP addresses of your clients after the router reboots with its new IP address.

> **Note**: The default LAN IP address of the router is **192.168.2.1** and default Subnet Mask is **255.255.255.0**.

IP Address

If you modify the router's IP address, your browser will continue to use the old IP address after you save your changes. This means that you will need to enter the router's new IP address in your browser after you save your changes in order to access the router again. (First you may have to release and renew the IP addresses of all devices connected to the router so they can acquire a new IP address and re-connect. You can find information about this in the user manual on the installation CD-ROM.)

IP address: `192.168.2.1`

Subnet mask: `255.255.255.0`

DHCP

The DHCP server can automatically assign IP addresses to wired and wireless clients that connect to the router.

DHCP Server

☑ DHCP server

IP range: `192.168.2.2` to `192.168.2.31`

Lease time: `0` days `1` hours `0` minutes

Domain name: ``

- **DHCP server**: When selected, the router will automatically assign IP addresses to clients that connect to the network. By default, this feature is enabled.

- **IP range**: The IP range of DHCP server also depends on the LAN subnet mask of the

router. The default range is 192.168.2.2 to 192.168.2.31.

To specify a different range for IP addresses, select IP address range and enter the starting and ending IP address.

- **Lease time**: You can set the Lease time for the assignment of IP addresses to network clients. This determines how long a client is allowed to use an assigned IP address. If a client is not active for a period of time and the lease expires, the IP address will be released and can be used for another client. The expired client will then have to send a request for an IP address the next time it attempts to connect to the network. You can change the length of the lease depending on how long you think a client should have an IP address. There is no need to change this setting unless you have a large network and you are short on available IP addresses to be assigned.

- **Domain name:** Specify the local network domain name which the router will use. Each host which receives an IP from the router's DHCP server will belong to this domain.

802.1d

The 802.1d spanning tree protocol is a management protocol that allows bridges within a network to communicate with each other to prevent loops within the network. This is enabled by default.

Static Routes

Static Routes

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

IP address: [   ]

Subnet mask: [   ]

Gateway: [   ]

Hops: [   ]

[Add]

If you connect the router to an existing network as the primary gateway to the Internet, or connect another router to this router, you may need to establish Static Routes. This will allow the clients that are not directly connected to the router to access the network resources of the router's LAN.

Note: The default LAN IP address of the router is **192.168.2.1** and default Subnet Mask is **255.255.255.0**.

1. Enter the IP address of the destination network/host in the **IP address** field.

2. Enter the Subnet mask for the destination host or network in the **Subnet mask** field. If you are adding a static route for a single host, this should be **255.255.255.255**.

3. Enter the Gateway the router will use to send traffic to the destination network/host in the **Gateway** field.

4. Enter the number of routers that this router must connect through in order to

connect to the other network in the **Hops** field.

The number of hops is determined by how many routers are between your router and the respective network.

Example: If there is another router connected to the router 's LAN port, you would enter **1** for the number of hops between the router's LAN port and any client connected to the second router.

5. Click **Add**.

Note: You need to click **Save** to save all your new settings and reboot the router after you have completed all your changes.
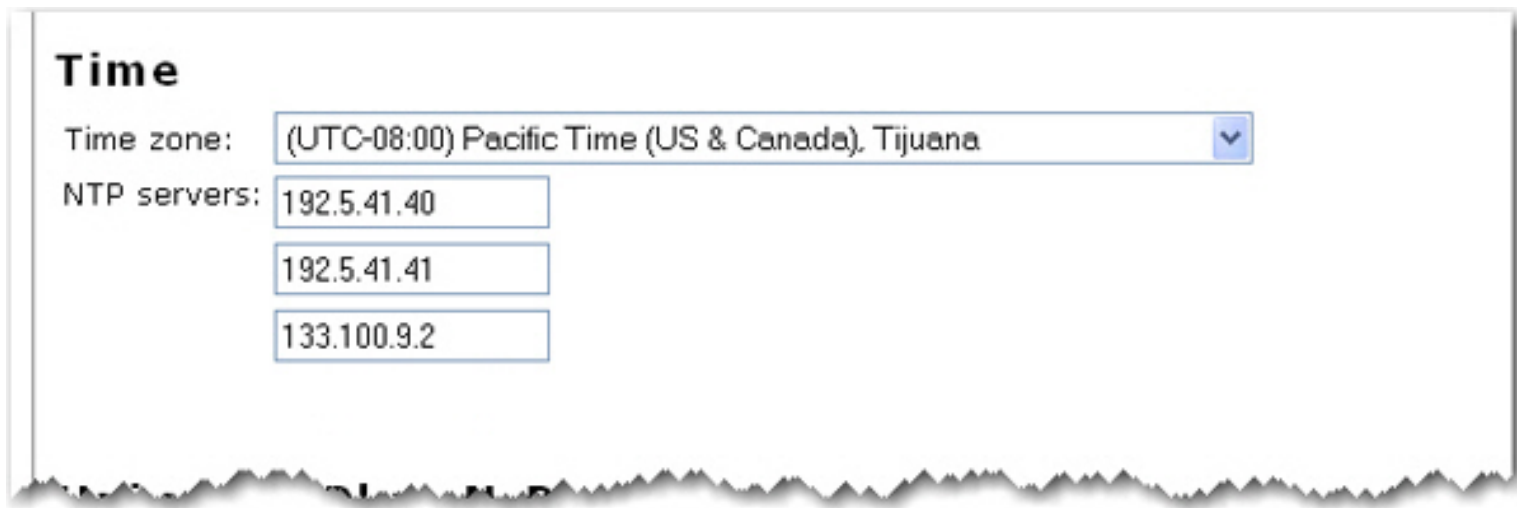

© 2006 U.S. Robotics Corporation

USRobotics *Wireless Nd1 Router User Guide*

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

Device Settings

In the router configuration pages, the **Device** page lets you access some of the basic settings of the router and perform administrative functions.

Time

The Time setting for your router apply to any firewall rules that you have in place. If you are using any firewall rules, you should set your Network Time Protocol (NTP) server and select your time zone.

Time

Time zone:	(UTC-08:00) Pacific Time (US & Canada), Tijuana
NTP servers:	192.5.41.40
	192.5.41.41
	133.100.9.2

1. Use the **Time zone** menu to select your time zone.

2. In the **NTP servers** fields, enter the domain or IP address of the NTP servers you wish to use.

3. Click the **Save** button to update your router with the time information from the NTP server.

Universal Plug-N-Play

Select **Universal Plug-N-Play** to enable Universal Plug-N-Play, or deselect it to disable the feature. After you change this setting, you need to click **Save** to apply the new settings to the router.

Reboot Router

If the router is not functioning properly, you can click **Reboot** to restart the router.

Upgrade Router

Firmware updates may be available on the USRobotics website to upgrade your device with new or improved features. If you are experiencing problems with your device, you may want to check for firmware updates.

1. Click **Check for Update** to search for the latest firmware from www.usr.com and save the firmware file to your computer.

2. Click **Browse** to locate and select the new firmware file.

3. Click **Upgrade** to begin the update process.

   The router may disconnect and reconnect to the Internet during the update. When complete, you will be prompted to log back in to the router.

   You should then see the new version of firmware listed on the Status page. If you do not, repeat the upgrade procedure.

Back up Settings

At any time, you can use Back Up Settings to save a backup file of your current router configuration, such as before you make significant changes to your router configuration, or after you have successfully applied changes.
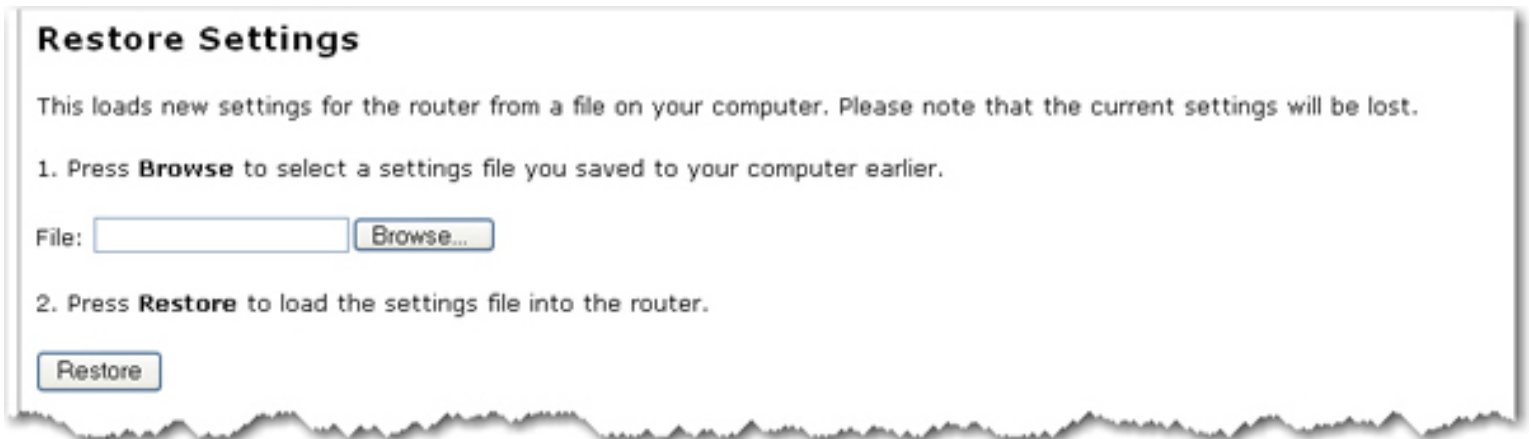

To save your settings:

1. Select **Back Up**.

2. A window appears. Click **Save.**

3. Browse to the location at which you want the backup file saved and click **Save.**

Restore Settings

If you ever lose your settings or if your settings have changed and the router is not functioning properly, you can restore your saved settings from a backup file. If you did not create a backup file, you may need to restore the default settings.

Restore Settings

This loads new settings for the router from a file on your computer. Please note that the current settings will be lost.

1. Press **Browse** to select a settings file you saved to your computer earlier.

File: [   ] [Browse...]

2. Press **Restore** to load the settings file into the router.

[Restore]

1. Browse to the location where your backup file is saved and click **Open.**

2. In the router configuration page, click **Restore**.

Factory Settings

Click **Reload** to restore the factory default settings of your router. When you restore the factory default, all your current settings will be lost. If you have forgotten the password to your router, you will need to restore to the factory default using the **Reset** button on the router, and then reinstall your router.

Factory Settings

This resets the router to its original factory settings. Please note that the current settings will be lost.

Reload

You can also restore the factory default settings using the **Reset** button on the router. Press in and hold the **Reset** button on the router for 7 seconds.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Frequently Asked Questions

Can I use SecureEasySetup to configure wireless security for my router?

Yes. For the initial setup of your router, refer to [installation instructions](#).

If you have a SecureEasySetup device already configured, you can set up wireless security on your router by performing the following:

1. Click the **SecureEasySetup** button on the back of your router.

2. Press the **SecureEasySetup** button in the utility for the client adapter. Your client adapter will display a message when the connection has been successfully completed..

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.

--- --- --- --- --- --- --- --- --- --- --- --- --- --- ---

What can I do if the specified installation procedure did not work?

1. Try unplugging the power supply of your cable or DSL modem then plugging it back in to reset it.
2. Restore the factory default settings of the router. Press in and hold the **Reset** button for between five and ten seconds. This will reset the router to the factory default settings. If you applied any personal configuration settings, you will need to make the changes again.

--- --- --- --- --- --- --- --- --- --- --- --- --- --- ---

What type of cable do I need to use to connect my broadband modem to the router ?

Some types of broadband modems require that you use a cross-over cable to connect to the router. Use the cables that were included with your router and with your broadband modem. Contact your ISP if you are still uncertain about which type of cable you must use.

--- --- --- --- --- --- --- --- --- --- --- --- --- --- ---

Does the router support IPSEC?

Yes, the router supports IPSEC pass-through.

What type of firewall is the router equipped with?

The router uses a Stateful Packet Inspection firewall for protection from network intrusions. The router uses NAT and TCP/IP port forwarding.

What is NAT?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This provides security since the IP address of a computer on the LAN is not transmitted to the Internet. The user can have multiple private addresses behind the single address that was provided by the ISP.

What is DMZ?

DMZ stands for Demilitarised Zone. This feature allows one IP address to be exposed to the Internet. DMZ allows only one computer to be exposed when multiple TCP/IP ports need to be open.

If DMZ is used, does the exposed user share the public IP with the router ?

No, all specific requests are forwarded to the DMZ host.

What should I do if I am unable to access my e-mail or the Web page of my

ISP?

You should contact your ISP to get the full URL and then complete the following steps:

> **Note:** Linux users can perform steps 4 and 5 after opening a terminal.

1. Connect your broadband modem directly to one of your computers.
2. Click Windows **Start** and then **Run**.
3. In the Run dialog box:
   Windows XP, 2000, and NT users: Type **cmd**.
   Windows Me, 98, and 95 users: Type **command**.
4. All users should then enter the following command: **ping xxx**, where *xxx* is the complete URL for your ISP.
5. After you get the IP address, enter the IP address in the mail server option or in the address line of your Web browser.

Are PPTP packets passed through or actively routed by the router ?

PPTP pass-through is supported if a PPTP client is used from one of the computers on the router's LAN. If the router's PPTP WAN interface is used, then the PPTP packets will be routed by the router.

What is the maximum number of users that the router will allow?

If you attach additional hubs to the router, up to 253 separate users can connect to the router.

Is the router compatible across different platforms?

Any platform that supports Ethernet, Wi-Fi compatible 802.11b and 802.11g products, and TCP/IP is compatible with the router.

Will the router allow me to use my own public IPs and domain, or do I have to use the IPs provided by the router ?

Only one valid Internet IP address is necessary. The internal IP address range will still go through the NAT firewall for all outbound Internet requests. All inbound requests will be blocked unless specific settings have been set up, such as port forwarding or DMZ.

How many ports can be forwarded at the same time?

You can use up to 30 Port Forwarding rules at the same time.

Can the router be used in place of a modem?

No, the router must be used with a broadband modem.

Is there a security log feature for the router ?

Yes, there is a security log feature in the configuration pages.

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

Support

1. Know your model and serial number.

   Your model number is 5464. You can find your serial number on the side of the package and on the bottom of the router.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support

   Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your router.

   The Support Web pages also contain information on the latest firmware and documentation updates.

3. Submit your technical support question using an online form, or contact the USRobotics Technical Support Department.

Country	Webmail	Voice
United States & Canada	http://www.usr.com/emailsupport	(888) 216-2850

Country	Webmail	Voice
Austria	www.usr.com/emailsupport/de	07110 900 116
Belgium (Flemish)	www.usr.com/emailsupport/nl	070 23 35 45

Belgium (French)	www.usr.com/emailsupport/be	070 23 35 46
Czech Republic	www.usr.com/emailsupport/cz	
Denmark	www.usr.com/emailsupport/ea	38323011
Finland	www.usr.com/emailsupport/ea	08 0091 3100
France	www.usr.com/emailsupport/fr	0825 070 693
Germany	www.usr.com/emailsupport/de	0180 567 1548
Greece	www.usr.com/emailsupport/gr	
Hungary	www.usr.com/emailsupport/hu	0180 567 1548
Ireland	www.usr.com/emailsupport/uk	1890 252 130
Italy	www.usr.com/emailsupport/it	800 979 266
Luxembourg	www.usr.com/emailsupport/be	342 080 8318
Middle East/Africa	www.usr.com/emailsupport/me	+44 870 844 4546
Netherlands	www.usr.com/emailsupport/nl	0900 202 5857
Norway	www.usr.com/emailsupport/ea	23 16 22 37
Poland	www.usr.com/emailsupport/pl	
Portugal	www.usr.com/emailsupport/pt	0 21 415 4034
Russia	www.usr.com/emailsupport/ru	8 800 200 20 01
Spain	www.usr.com/emailsupport/es	902 117964
Sweden	www.usr.com/emailsupport/se	08 5016 3205
Switzerland	www.usr.com/emailsupport/de	0848 840 200
Turkey	www.usr.com/emailsupport/tk	0212 444 4 877
United Arab Emirates	www.usr.com/emailsupport/me	0800 877 63
United Kingdom	www.usr.com/emailsupport/uk	0870 844 4546

For current support contact information, go to: www.usr.com/emailsupport

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

- Home
- Installation
- Configuration
- Tutorials
- Help

Basic Troubleshooting Procedure

This procedure addresses a number of symptoms that you might experience with your router and wireless connection:

1. Verify the physical cable connections between your router, your computer, and your modem.

2. Ensure that the power outlet to which the router is connected is a live outlet.

3. Refer to the LED descriptions and then check the LEDs on the router to make sure you are receiving power and that are no errors.

4. Reboot your router to refresh your Internet connection information.

5. Some electronic devices, such as 2.4GHz - 5.8 GHz phones and microwave ovens, may interfere with the wireless signal and affect your wireless range and link quality. Try creating a wireless connection on a different channel.

6. Low link quality or range can be caused by environmental interference, such as lead-based paint and concrete walls. Try to move the antenna of the router or to reposition the wireless clients to improve the link quality. If possible, ensure that there are no obstructions between wireless clients and the router.

7. Go to the **Status** page of the configuration pages and use the **Network Test**

(Ping) to verify communications between your computer, your router and the Internet.

If you still have trouble using the router, follow the procedure below that best describes your symptom.

Router Installation and Configuration

The Setup Wizard was unable to detect my Internet connection.

My wireless card does not support WPA, can I still secure my network?

I do not remember my wireless security settings.

I do not know if my IP Address from my ISP is Static or Dynamic.

I can't connect to the router configuration pages.

My router configuration pages are not responding, but I can still access the Internet.

My router is not responding after I performed a firmware upgrade.

I accidentally blocked all wireless devices from accessing the router.

Internet and Wireless Connections

SecureEasySetup could not configure my wireless client.

I am no longer able to access the Internet.

My wireless adapter cannot connect to the router.

I cannot achieve 270 Mbps connections to the Wireless **N**d_1 Router.

My router is not appearing in the list when my wireless adapter scans for it.

I can access the Internet through the router but cannot access some special applications.

After enabling VPN, I am unable to connect to local computers on my network to share files or printing capabilities.

I am experiencing poor wireless link quality.

Printing

[I cannot print to a network printer attached to my router in Windows XP or 2000](#)

[I cannot print to a network printer attached to my router in Windows Me or 98SE](#)

[I cannot print to a network printer attached to my router in Macintosh OS 9 or earlier](#)

[Documents printed using the print server on the router do not begin immediately and sometimes take one minute or longer to begin printing.](#)

[My scanner is not working.](#)

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

The Setup Wizard was unable to detect my Internet connection.

You will need to manually configure your Internet connection. There are two methods of instructions you can follow to setup your Internet connection.

If you are still in the Setup Wizard:

1. Do one of the following:

   ❍ Verify the power cord and all the Ethernet cables are <u>connected correctly</u>, then press **Detect Connection** to attempt the automatic configuration of your Internet connection.

   ❍ Manually configure your connection by selecting your Internet connection type: either **Cable, DSL router, satellite, ISDN, LAN, or other** or **DSL modem (also known as PPPoE)** and any information required by you ISP.

2. Click **Next** and continue to follow the on-screen instructions to complete the Setup Wizard.

If you have already closed the Setup Wizard:

1. Launch a Web browser.

2. In the location or address line of your Web browser, type **192.168.2.1** to access the router configuration pages.

3. Click the **Internet** tab.

4. Select your Internet connection type: either **Cable, DSL router, satellite, ISDN, LAN, or other** or **DSL modem (also known as PPPoE)** and any information required by you ISP.

5. When you are finished, click **Save**. You should now be able to access the Internet.

Return to Troubleshooting page

© 2006 U.S. Robotics Corporation

USRobotics® *Wireless Nd1 Router User Guide*

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

I am no longer able to access the Internet.

When your computer connects to the Internet using the router, a number of devices have to work together.

- Your computer connects to your router via a wireless or wired connection.

- Your router connects to your broadband cable/DSL modem via an Ethernet cable.

- Your cable/DSL modem connects to your Internet Service Provider (ISP) via your cable/ phone network.

The first step in solving this problem is to diagnose the cause. There are a number of places where the connection from your computer to the Internet might fail.

Check the indicator lights of your various devices. If one or more of these devices indicate a problem, it's a good indication of where you should focus your troubleshooting efforts.

If you still cannot connect to the internet, manually step through the following procedures.

1. Verify the wired or wireless connection to your router. If your computer cannot communicate with the router, it cannot access the Internet.

2. If the LEDs for your router **are not** responding, verify your router is responding. This

includes checking the LEDs to verify they are functioning correctly and to verify that the router is powered on responding. If the router is turned off, or the wireless radio isn't operating, or it has no connection to the Internet (via your cable/DSL modem), your computer won't be able to access the Internet either.

3. If the LEDs for your router **are** responding, verify your router's connection to the Cable or DSL modem. Your router must be connected to and receiving information from the modem for a successful Internet connection.

4. Verify your modem's connection to the Internet. Your Internet connection must be up and functioning.

Verify the wired or wireless connection to your router

If you use a wired connection:

1. If you use a wired connection between your computer and your router, ensure the Ethernet cable is securely connected to your computer's Ethernet port and to a LAN port on the router.

2. Verify that the corresponding LED for the LAN port is lit. Make sure your computer has an IP address in the same subnet as the router. If you still cannot get to the Internet, verify your router is responding.

If you use a wireless connection:

1. If you use a wireless connection between your computer and your router, ensure the wireless utility reports a successful connection to your router.

2. Ensure that your computer is connected to your router, and not another router like a neighbor's router. You can use your wireless utility to check the **Network name** (SSID) of the router you're connected to. If it's connected to the wrong router, you can use the utility to force your computer to try to connect to your router. See the documentation of your wireless adapter for information on how to check which router you are connecting to.

If you do not have a wireless connection to your router:

1. Ensure that your computer is close enough to your router to receive a signal and that there is nothing interfering with the signal, such as a microwave oven or a concrete wall. If your perform a scan with your wireless utility (typically called a "site survey") and it can't detect your router, it may be a signal problem.

2. Verify your router is configured to broadcasts its network name.

3. Ensure that the wireless utility is using the correct **Network name** (SSID) and <u>wireless security settings</u> for your router.

   Settings such as network name, security method (WPA, WEP, etc.), and security keys must all match. If your router is using WPA encryption, each wireless card or adapter must support WPA encryption. If you are using a Wireless PC Card, PCI adapter, or USB adapter that does not support WPA encryption, you will not be able to connect to the router and will need to use WEP encryption. Please refer to the Configuration section of this User Guide for information on changing the security settings.

4. Verify the computer permitted to connect to your router. If you have MAC filtering enabled on your router, you should verify that the MAC address of your wireless adapter is allowed access to the router. For example, if you have changed wireless adapters, you will have to add the MAC address of the new wireless adapter to the router.

5. If none of these work, you can try a wired connection between your computer and your router by connecting an Ethernet cable between your computer's LAN port and a LAN port on the router. (Ensure that the corresponding LAN port LEDs are lit.) If a wired connection works, the problem is almost certainly with your computer's wireless connection to the router. You should then try the previous steps again.

If you can verify the connection between your computer and your router, it's likely the router is not connected to the Internet or is not functioning correctly. You need to <u>verify your router's connection to the Cable or DSL modem</u> and <u>verify your modem's connection to the Internet</u>.

Verify your router is responding

1. Check that the router's LEDs for power, wireless, and Internet are lit.

2. Start a Web browser. In the location or address line type **192.168.2.1** and press ENTER.

> **Note**: If you have modified your router's IP address, enter the new IP address instead of 192.168.2.1.

If the router's Web interface appears and you still cannot connect to the Internet, the problem may be with its connection to your cable/DSL modem. Go to Step 3.

If the router's Web interface doesn't appear, you should release and renew your computer's network connection.

Release and renew your computer's network connection.

1. Do one of the following:

   Windows XP, 2000, and NT users:

   Go to Windows **Start** > **Run**.

   Type **cmd** and press ENTER.

   Type **ipconfig /renew** and press ENTER.

   Type **exit** and press ENTER.

   Windows Me, 98, and 95 users:

   Go to Windows **Start** > **Run**.

   Enter **winipcfg** and press ENTER.

   Press **Release**.

Press **Renew**.

Close the application.

2. Your computer should acquire an IP address (such as 192.168.2.5) from the router.

3. Try again to access the router configuration pages at **192.168.2.1**.

4. If the router configuration pages appear and you still cannot connect to the Internet, the problem may be with its connection to your cable/DSL modem. Verify your router's connection to the Cable or DSL modem.

5. If the router configuration pages still do not appear, you need to restart your router.

   A. With a thin tool, such as a paper clip, briefly press the **Reset** button on the back of the router for 1 second.

   > **Note:** If you press the **Reset** button for more than five seconds, the router will return to its factory default settings.

   B. Wait about 30 seconds for the LEDs on the router to stabilize.

   C. Release and renew your computer's network connection information again.

   D. Try again to access the router's Web address at **192.168.2.1**

   E. If the router configuration pages appear and you still cannot connect to the Internet, the problem may be with its connection to your cable/DSL modem. Verify your router's connection to the Cable or DSL modem.

6. If you still cannot access the router, the router may need to be restored to the default factory settings.

   > **Note:** When you restore to the factory default settings, you will lose all of your router's custom settings and will need to set it up again as if you were

installing it for the first time. Alternatively, you can restore your settings if you have made a backup of your router settings.

A. With a thin tool, such as a paper clip, press the **Reset** button on the back of the router for 7 seconds.

B. Wait about 30 seconds for the LEDs on the router to stabilize.

C. Try to access the router's Web address at **192.168.2.1**

D. If the router's Web interface still doesn't appear after you have restored to the factory default settings, it's possible that the router has failed. Please contact U. S. Robotics Customer Support.

Verify your router's connection to the Cable or DSL modem

1. Check your cable/DSL modem's power and status LEDs to verify that the modem is powered on and connected to the Internet. Refer to your modem's documentation for information on its status indicators.

2. In the router configuration pages, click the **Status** tab.

3. Click **Refresh** to update the page with the most current status information.

4. Go to the **WAN** section of the page and verify that the router has a WAN IP address (such as 235.42.181.5). This IP address indicates whether the router is connected to the cable/DSL modem.

5. If the router doesn't have a WAN IP address, reboot the router.

6. If you still cannot access the Internet, click the **Internet** tab and use the page to configure the router's Internet connection. (If you have a DSL modem, you may be required to enter the login information your ISP provided.)

> **Note:** If the WAN protocol is static, you will need to make sure the WAN IP address of the router is a valid static IP address. A valid static IP address is one that is provided by your ISP or is in the same subnet as the device that is connected to the WAN port of the router.

7. If the router still cannot obtain a WAN IP address, it is likely there is a problem with the cable/DSL modem or your ISP. Verify your modem's connection to the Internet.

Verify your modem's connection to the Internet

If your computer has a connection to your router and the Internet connection information on your router is configured correctly but you still cannot connect to the Internet, it's possible that the cable/DSL modem has lost its connection or isn't functioning properly, or there's a problem with your ISP.

1. Ensure that an Ethernet cable is connected between your router's WAN port and the cable/DSL modem's Ethernet port and that the corresponding LEDs are lit.

2. Ensure that your cable/DSL modem is connected to your wall jack. (A cable modem uses a coax cable, and a DSL modem uses an RJ-11 cable.)

3. Restart your cable/DSL modem. (There may be a power switch or reset button on the modem or you may have to unplug/re-plug the modem's power adapter. Consult your modem's documentation.)

4. After the cable/DSL modem has restarted and connected to your ISP, click the **Reboot** button on your router's **Device** page.