USER GUIDE

HomePortal Intelligent Gateway

5268ac

BRINGING TECHNOLOGY HOME

www.pace.com

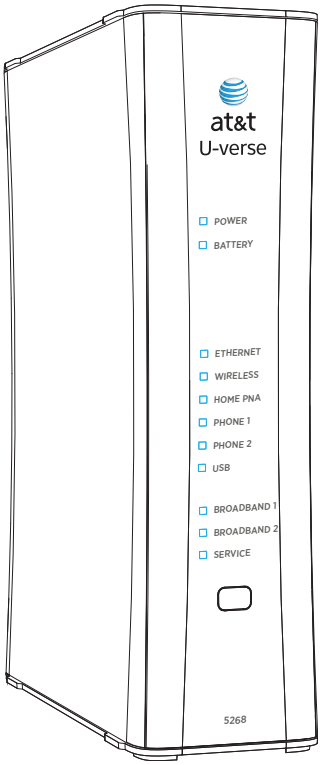
04292014

504-3315420

Contents

Introduction 1

The Home Portal® Intelligent Gateway is an advanced networking device that can be installed by you or your service provider. This all-in-one device includes the modem, router, wireless access point, firewall, and backup battery.



The gateway supports ADSL, ADSL2, ADSL2+, and VDSL2 technology. It has four wired Ethernet ports and 802.11b/g/n/ac wireless networking.

Pace wireless technology practically eliminates wireless “cold spots” in the home. Increased power and sensitivity, along with optimized antenna design, give better range and performance than typical wireless access points.

With its fully configurable and manageable firewall, the Pace gateway provides firewall protection for up to 253 networked devices without affecting routing speed. The firewall actively detects and defends against common Internet threats using stateful packet inspection. It is easy to configure for common applications such as online gaming.

Status lights

Use the status lights on the front of the gateway to determine its current state.

Status light	Description
Power	• *Solid green*. The gateway is on. • *Red*. The gateway may have a fault with its power supply.
Battery	• *Solid green*. The backup battery is installed but the gateway is not currently using battery power. • *Flashing green*. The battery is charging. • *Solid red*. The battery is faulty. • *Flashing red*. The battery should be replaced. • *Solid amber*. The gateway is using battery power. • *Flashing amber*. The battery is low. • *Off*. No battery is installed or the battery has no charge. • *Alternating colors*. The battery is conducting a self-test.
Ethernet	• *Solid green*. A computer or other device is connected to an Ethernet port. • *Flickering green*. There is activity from devices connected to an Ethernet port. The flickering of the light is synchronized to data traffic.
Wireless	• *Solid green*. A wireless computer or other device is connected to the gateway. • *Flickering green*. There is inbound or outbound activity. The flickering of the light is synchronized to data traffic.
Home PNA	• *Solid green*. A set-top box or other device is connected to the coaxial port. • *Flickering green*. There is activity from devices connected to the coaxial port. The flickering of the light is synchronized to data traffic.
Voice 1 Voice 2	• *Solid green*. A phone is connected. • *Flashing green*. The associated phone is active.
USB	• *Solid green*. A device is connected to the USB port. • *Flashing green*. The USB device is active.
Broadband 1 Broadband 2	• *Solid green*. The gateway is connected to the provider network. • *Flashing green*. The gateway is trying to connect to the service provider network. The light might flash for a few moments while the gateway connects. • *Flashing green and red*. The gateway has been trying to connect to the service provider network for more than three minutes. See “Connection issues” on page 24. • *Flashing red*. The gateway cannot connect to service provider network or no DSL signal is detected. See “Connection issues” on page 24. • *Off*. The gateway is turned off or the associated line is not connected or not in use.
Service	• *Solid green*. The gateway is connected to the service provider network and has obtained a WAN IP address. • *Fast flashing green*. The gateway is trying to obtain an IP address. • *Red*. The service provider network is not responding, the gateway has been configured incorrectly, or there was an authentication failure.
WPS	• *Solid green*. WPS (Wi-Fi Protected Setup) is configuring the gateway.

Setting up the Gateway 2

Before you install the gateway, find an appropriate location for it. Set up the gateway near the main computer or any other device that will connect to it through the wired Ethernet ports.

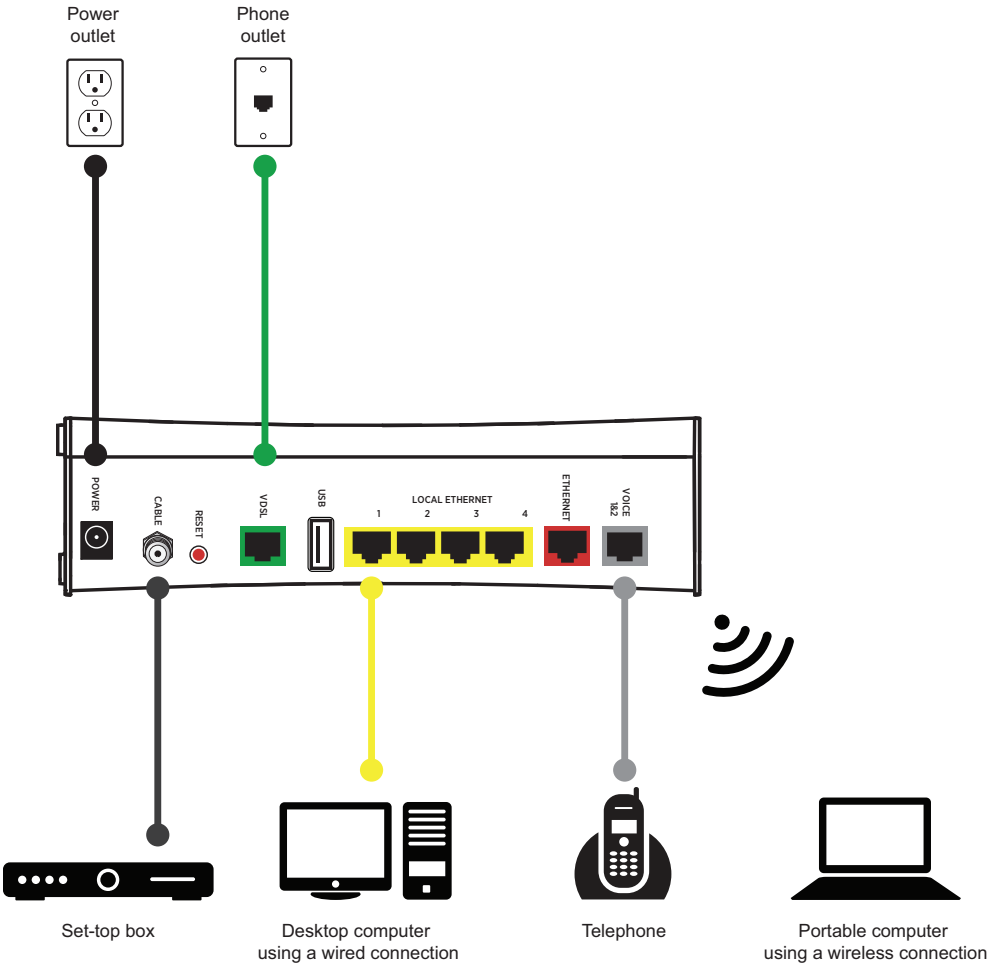
The gateway also serves as a wireless access point, so you should consider the wireless network when choosing the location for the gateway. Consider the following when determining the location of the gateway:

- Place the gateway at least 5 ft (1.5 m) from cordless phones, microwave ovens, or other electronic devices to avoid potential interference, and at least 6 in (15 cm) from your television to avoid audio hissing or static.
- Place the gateway in an open area to minimize interference from its surroundings. Wireless signal strength is much stronger in an open area than an area with obstructions. In a single-story building, place the gateway as high and as close to each wireless device as possible.
- Keep the gateway away from large metal objects. Metal objects can reflect or obstruct signals, which can negatively impact wireless signal quality.
- Place the gateway in an open area to allow for proper ventilation.
- Keep the gateway away from water sources like water coolers or aquariums.

Note: We recommend that you use the included stand to install the gateway vertically. This prevents things from being stacked on top of it, which can block vents and cause the gateway to overheat.

Connection overview

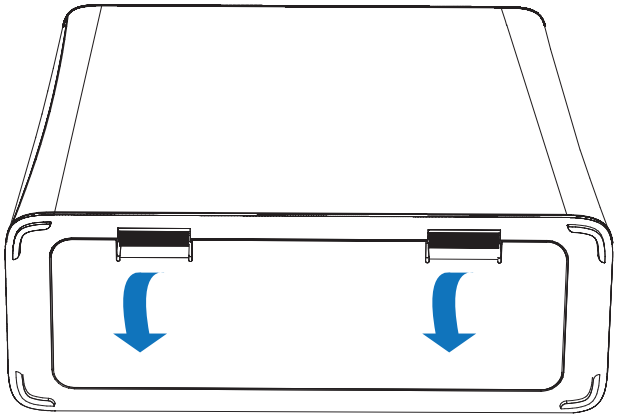
Connect the gateway to the DSL line, and connect devices to the gateway using a wired or wireless connection. The following illustration shows on overview of the connections.



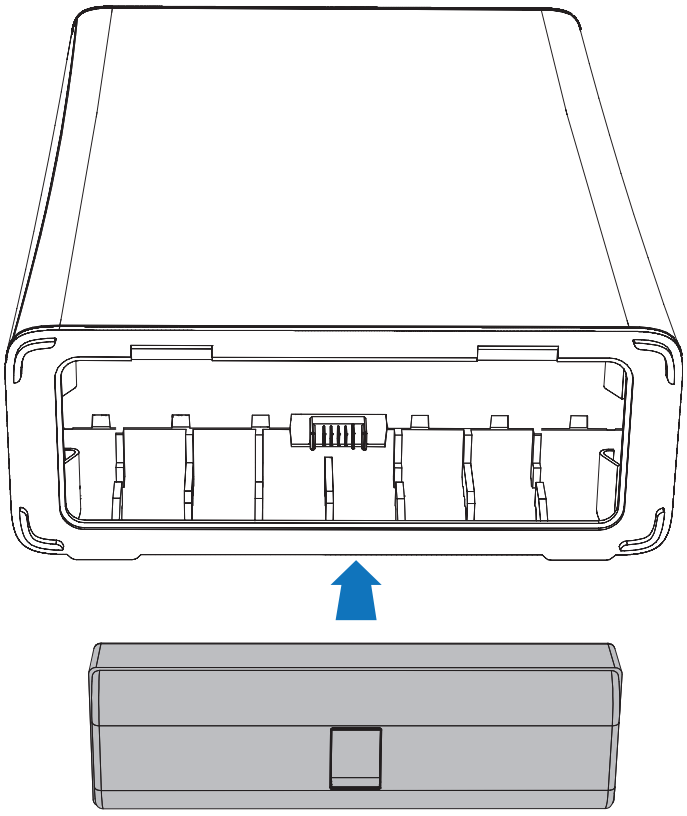
Inserting the battery

The gateway includes an integrated battery. The battery provides backup power in case of power failure. You should insert the battery before you use the gateway.

1. Open the battery door.



2. Insert the battery into the battery compartment.



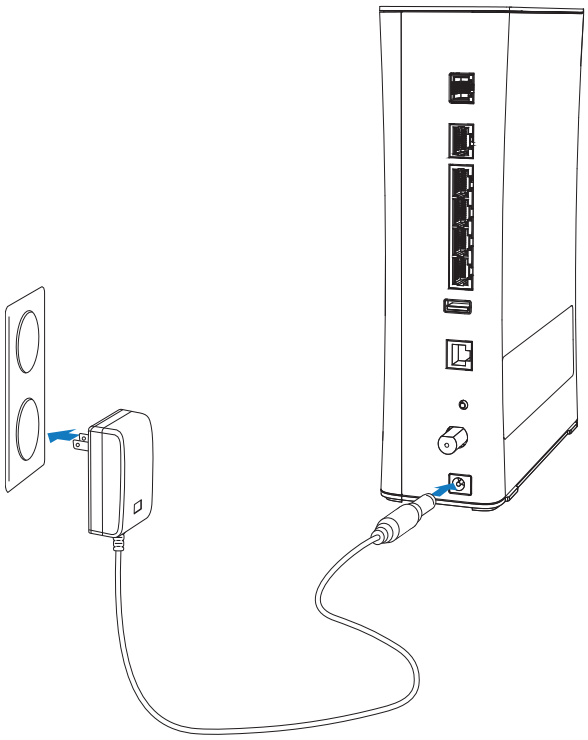
3. Close the battery door.

Connecting the power adapter

Use the power adapter that was packaged with the gateway because it matches the power requirements of the gateway and it complies with local requirements.

1. Connect one end of the power adapter to the POWER port on the gateway.
2. Connect the other end to a power outlet.

After the gateway is powered on, the power light blinks green for a moment and then turns steady green.



Connecting the gateway to the Internet

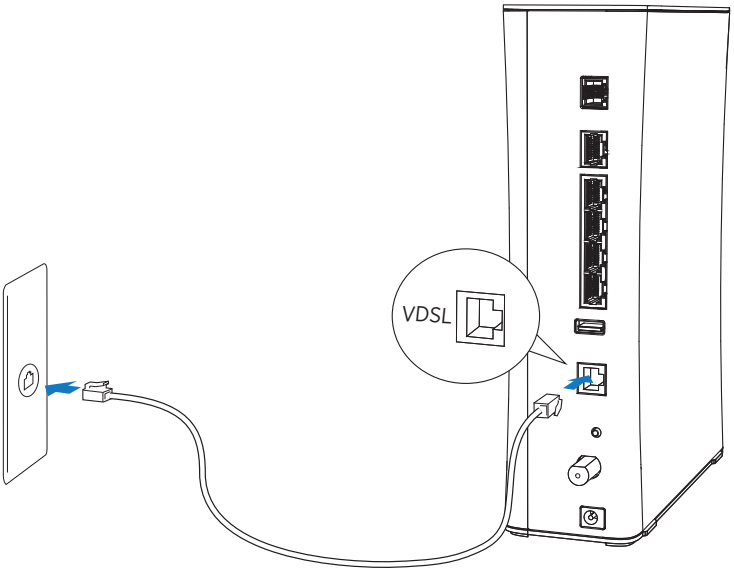
You can connect the gateway to the Internet using the DSL port or the Ethernet port.

Using the VDSL port

Connect the gateway to the Internet through the VDSL port.

1. Connect one end of a phone cord to the green VDSL port on the gateway.
2. Connect the other end of the phone cord to the phone outlet.

After the gateway recognizes the connection, the Broadband light blinks green for a moment and then turns steady green.



Using the Ethernet port

If directed by your service provider, you can connect the gateway to the Internet through the Ethernet port.

1. Connect one end of an Ethernet cable to the Ethernet port on the gateway.
2. Connect the other end of the Ethernet cable to the broadband device.

After the gateway recognizes the connection, the Broadband light blinks green for a moment and then turns steady green.

Connecting devices to the gateway

You can connect your computers and devices to the gateway using a wired or wireless connection. With either type of connection, you can use the first computer that you connect to the network to set up the gateway.

Using a wired connection

The gateway has four wired Ethernet ports that you can use to connect computers or other devices.

1. Connect one end of the yellow Ethernet cable to one of the yellow Ethernet ports on the gateway.
2. Connect the other end of the cable to the Ethernet port on the computer.

You can connect up to four computers to the gateway using the wired Ethernet ports.

Note: A 6-foot yellow Ethernet cable is provided with the gateway. If you need another cable, use a Cat 5 or Cat 5e Ethernet cable.

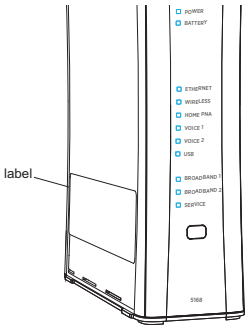
After the gateway recognizes the computer, the Ethernet light turns steady green, and blinks when the computer starts transferring data with the gateway.

Using a wireless connection

The gateway has an integrated wireless access point that you can use to connect wireless devices to the gateway. By default, the gateway is configured with a network name (SSID) and WPA-PSK/WPA2-PSK security.

1. On the wireless device, view the available wireless networks. The specifics of how you do this depend on the device you are connecting.

   The SSID (default wireless network name) and wireless network key are printed on the label on the side of the gateway. Mac OS X users might have to enter the "$" character at the beginning of the encryption key.



2. Select the appropriate wireless network name and connect.
3. At the prompt, enter the wireless network key.

After the gateway recognizes the wireless device, the Wireless light turns steady green, and blinks when the wireless device starts transferring data with the gateway.

Connecting VoIP telephones

The gateway includes one RJ-14 port (Voice 1 & 2) with the capacity to support 2 phone lines using a splitter or multi-jack adapter.

WARNING: Do not connect the VoIP lines to your current home telephone wiring, especially if your home has an alarm system. Ensure that you are subscribed to voice service before using the voice lines on the gateway.

1. Connect one end of the phone cable to the gray Voice 1 & 2 port on the gateway.
2. Do one of the following:
   - For one phone, connect the phone cable directly to the telephone.
   - For two phones, connect the phone cable to a splitter and then to the phones.

Note: To prevent interference with cordless phones, ensure that the gateway is at least 5 feet (1.5 m) from the cordless phone base station.

After the gateway recognizes a phone, the corresponding status lights (Voice 1 and Voice 2) turn steady green and blink when the associated phone is active.

Connecting an IPTV set-top box

You can connect an IPTV set-top box to the gateway for television service.

1. Connect one end of the coaxial cable to the Cable port on the gateway.
2. Connect the other end of the coaxial cable to the Cable input (Video in) port on the set-top box.

After the gateway recognizes the set-top box, the Home PNA light turns steady green, and blinks when the set-top box starts transferring data with the gateway.

Note: For more information, see the instructions that came with the set-top box.

Installing DSL filters

The DSL signal is carried over the same lines as the regular phone signal. Converting your regular phone line to DSL can cause high-pitched tones and static when you use the phone. To eliminate the noise, install DSL filters on every phone or phone device that shares the same phone number as the DSL service.

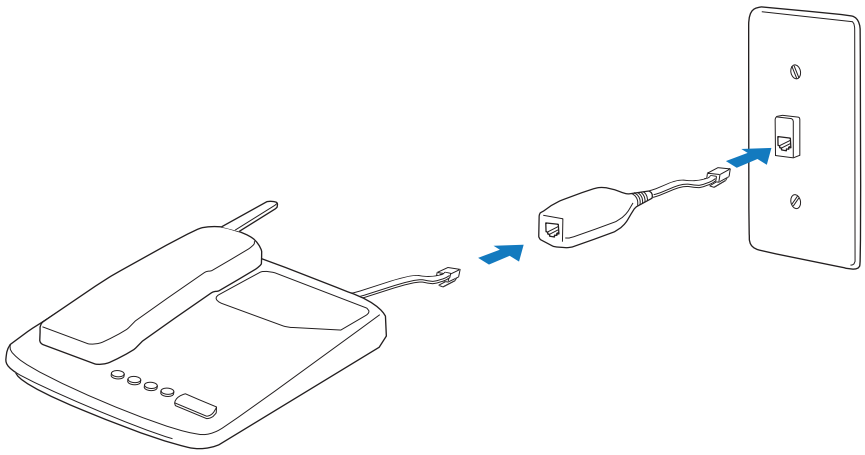
You need one DSL filter for each phone device (such as a desktop phone, analog modem, Fax, or answering machine). If you have several phone devices connected to each other and are using a single phone jack, install only one DSL filter between the phone jack and the first device in the series.

Important: Do not install a DSL filter on the line that is connected to the DSL gateway.

Installing a DSL inline filter

For most phones, you should install the DSL filter between the device and the phone jack.

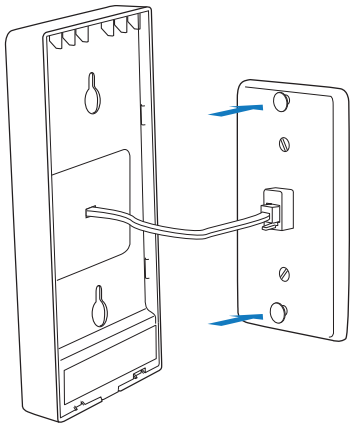
1. Connect the cable from the phone to the DSL filter.
2. Connect the cable from the DSL filter to the phone jack.



Installing a DSL wall filter

For a wall-mounted DSL filter, install the DSL filter between the original wall plate and the wall-mounted phone.

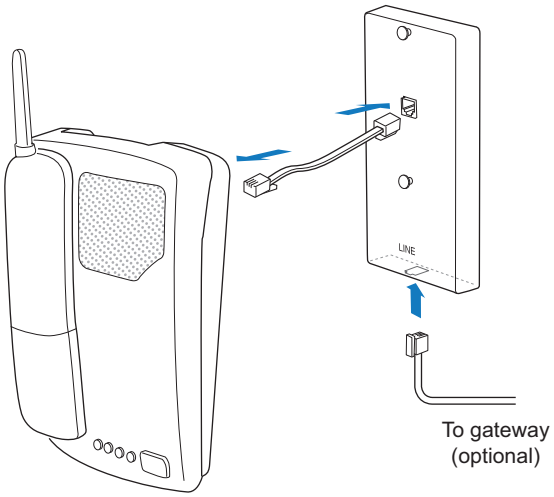
1. Lift the phone from the wall pegs, and disconnect the phone cord from the phone jack.
2. Connect the phone cord from the back of the DSL filter into the phone jack, and mount the filter on the wall plate pegs using the keyhole slots.



3. Connect the phone cable to the phone jack located on the front of the mounted DSL filter.

   Note: If you have a DSL gateway, you can connect it to the DSL port at the bottom of the filter.

4. Attach the phone to the mounting pegs on the DSL filter.



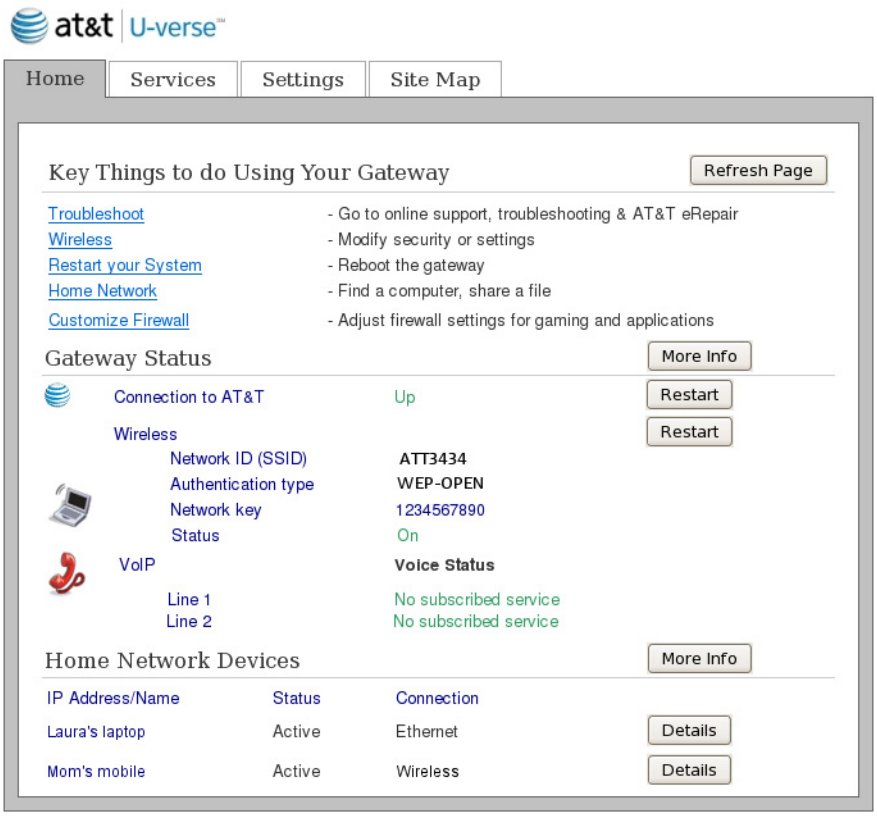
Configuring the Gateway 3

The gateway is configured automatically by your service provider, but you can change certain settings, such as the wireless network name, password, and firewall options.

Opening the gateway home page

Use the gateway home page to change settings on your gateway.

1. Start your web browser.
2. In the address bar, enter http://192.168.1.254.



You can also use http://gateway.pace.com to open the gateway home page.

Configuring general settings

You can configure common gateway settings, such as password and network name. Most users will not need to change anything other than the general settings.

Viewing system information

The System Information page shows details about the gateway, such as model number, serial number, and version information.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **System Info** tab.

Changing the system password

The system password controls access to the gateway configuration pages. You can use the default system password, or create your own. The default system password (Device Access Code) is printed on a label on the gateway.

If you create a custom password, you can also create a password hint to remind you of your password if you forget it.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **System Info** tab.
3. Click **Password**.
4. For **Enter Current Password**, enter the system password. The default system password (Device Access Code) is printed on a label on the gateway.
5. Select **Create or Edit a Custom Password**.
6. Enter the following information:
   - **Enter New Password**. The new password. The password is case-sensitive and can contain a maximum of 31 alpha-numeric characters and no spaces.
   - **Confirm New Password**. Re-enter the new password.
   - **Enter a Password Hint**. (optional) Enter a hint to remind you of your password if you forget it.
7. Click **Save**.

Changing the type of wireless security

You can change the type of security protocol that is used to protect your wireless network. WPA-PSK/WPA2-PSK security is enabled by default. We recommend that you do not disable it, because doing so can compromise the security of data transmitted over the wireless link.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **LAN** tab.
3. Click **Wireless**.

4. For **Authentication Type**, choose one of the following:
    - **WEP-Open**. Wireless Encryption Protocol (WEP) is an older security protocol that allows any wireless clients within the radio range to access your network without an encryption key. This setting provides the least level of security. For security reasons, do not select this setting unless there is a compatibility issue with an older wireless client.
    - **WEP-Shared**. Similar to WEP-Open, do not select this setting unless there is a compatibility issue with an older wireless device. Unlike WEP-Open, WEP-Shared prevents open access by any wireless device; therefore, it is more secure than WEP-Open.
    - **WPA-PSK (TKIP)**. Wi-Fi Protected Access - Pre-Shared Key provides good security and works with most wireless devices. This setting requires an encryption key to be set on the gateway and on the wireless device.
    - **WPA-PSK (TKIP) and WPA2-PSK (AES)**. This setting allows a wireless device to use either WPA-PSK or WPA2-PSK to access your wireless network. This setting requires an encryption key to be set on the gateway and on the wireless device.
    - **WPA2-PSK (AES)**. This setting requires that wireless devices use only WPA2-PSK to access your networks. WPA2-PSK is currently the most secure Wi-Fi encryption protocol but may not be available on all wireless devices. This setting requires an encryption key to be set on the gateway and on the wireless device.
5. Click **Save**.

Changing the wireless password

The wireless password controls access to the wireless network. You can use the default password or choose your own. The default wireless password (Wireless Network Key) is printed on a label on the gateway.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **LAN** tab.
3. Click **Wireless**.
4. Select **Use Custom Wireless Network Key**.
5. Enter the password you would like to use.
6. Click **Save**.

Changing the network name

The network name, or SSID, is the name users will see when they try to join your wireless network.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **LAN** tab.
3. Click **Wireless**.
4. For **Network Name (SSID)**, enter the name you would like to use for the wireless network.
5. Click **Save**.

Setting up event notifications

With event notifications, you will be notified if various service conditions or events occur. You will be redirected to a Web browser that will give you more information about the condition and provide potential solutions.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Event Notifications** tab.
3. Select the events for which you want to be notified.
4. Click **Save**.

Configuring broadband settings

Typically, your broadband settings are automatically configured by your service provider. When the gateway is connected, it detects which DSL line to use and does not require further configuration.

Use the information in this section if you want to configure the DSL and Internet connection settings manually.

Viewing broadband settings

The broadband settings page shows details about the WAN connection, such as connectivity status, Internet connection details, modem type, and traffic statistics.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Broadband** tab.
3. Click **Status**.

Configuring a publicly routed subnet

You can create a local network that has broadband network-accessible IP addresses by creating a route from the Internet to the specified public network. This feature is typically used with broadband service that provides a range of available IP addresses. Once enabled, the public IP addresses can be assigned to local computers.

Set up the LAN publicly routed subnet first if you want to use the public address with your DHCP configuration.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Broadband** tab.
3. Click **Link Configuration**.
4. Under **Supplementary Network**, locate **Add Additional Network**, and click **Enable**.
5. Enter the following information:
   - **Router Address**. The router IP address for the secondary subnet, provided by the service provider.
   - **Subnet Mask**. The router mask for the secondary subnet, provided by the service provider.
   - **Auto Firewall Open**. (optional) Disables the firewall for all devices using addresses from this subnet. The firewall is enabled by default.

     You can enable the firewall individually per device (See “Allocating IP addresses” on page 20) or per application (“Allowing all applications (DMZplus)” on page 23).
6. Click **Save**.

Configuring LAN settings

Typically, your Internet service provider automatically assigns and configures an IP address when the gateway connects to the Internet. Advanced users can use a static IP address that allows them to run services like file servers or mail servers. Service providers typically offer static IP addresses as an extra service.

Change these settings only if you are familiar with networking concepts.

Configuring DHCP

DHCP (Dynamic Host Configuration Protocol) allows network addresses to be allocated dynamically as needed. The gateway can be both a DHCP client and DHCP server. The gateway is a DHCP client because it obtains an IP address from the service provider over the Internet. The gateway is a DHCP server because it assigns IP addresses to the devices in your home network.

If you change the local network IP address range, you must renew the DHCP lease on devices connected to the home network and manually reconfigure all devices configured with static IP addresses.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then the **LAN** tab.
3. Click **DHCP**.
4. For **DHCP Network Range**, select an IP address range or select **Configure manually** to set up a custom range for the DHCP IP address pool.
5. If you selected **Configure manually**, enter the following information:
   - **Router Address**. The LAN IP address of the gateway.
   - **Subnet Mask**. The subnet mask of the gateway (default: 255.255.255.0).
   - **First DHCP Address**. The first IP address in the DHCP IP address pool to be assigned on the local network.
   - **Last DHCP Address**. The last IP address in the DHCP IP address pool to be assigned on the local network.
6. For **DHCP Lease Time**, enter the number of hours a device can use an assigned IP address before it expires.
7. For **New Device DHCP Pool**, select **Private Network** or **Public Network**. Use Public IP addresses only with DMZplus or a secondary subnet that allows you to have public IP addresses routed through the device.
8. Click **Save**.

Allocating IP addresses

You can allocate specific IP addresses to devices that are configured with DHCP, and map devices to particular static IP addresses. For Internet public hosting of application or servers associated with static addresses, you can map a device to a specific public static IP address or to the next unassigned address from the public pool. The default public IP device mapping is to the Router WAN IP address.

Alternatively, you can configure static public or private IP addresses on the devices themselves. Static IP addresses on devices override settings on this page.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **LAN** tab.
3. Click **IP Address Allocation**. The page shows the devices in your network.

4. Go to the appropriate device and select the following options to override the default DHCP settings:
   - **Firewall**. Determines whether the gateway firewall is enabled for the device.
   - **Address Assignment**. A specific address or address type.
   - **WAN IP Mapping**. The address or address pool from which you want to select an IP address.
5. Click **Save**.

Configuring firewall settings

The gateway's default firewall settings block unwanted access from the Internet. Most users will not need to change the default firewall settings.

If necessary, you can modify the firewall settings to allow certain Internet traffic or users through the firewall to devices on your home network.

Hosting an application

To allow access from the Internet to applications running on computers inside your home network, you need to open firewall pinholes and associate the intended application with a computer connected with your gateway. If you cannot find a listing for your application, you can define an application with the protocol and port information. For more information, see "Defining an application profile" on page 22.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Firewall** tab.
3. Click **Applications, Pinholes and DMZ**.
4. Select the computer that will host the application.

   If the computer you want to select is unlisted because it is powered off and the Hide inactive devices option is enabled, you can select it if it is on the same network and you know its IP address. Enter the IP address and click **Choose**.
5. Select **Allow individual application(s)**.
6. From the Application List panel, select the application you want to host.

   You can filter the application list by selecting a category.

   To select multiple applications, hold down the [Shift] or [Ctrl] keys while making your selections. Using the [Shift] key lets you make your selections in a contiguous order while the [Ctrl] key selects the groups in any order.
7. Click **Add**.
8. Click **Save**.

Defining an application profile

An application profile allows application-specific data to pass through the firewall. You can define an application profile that is not included in the application list. This feature is typically used if the application for which you would like to pass through data to a given computer is new or has been recently updated to a new version.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Firewall** tab.
3. Click **Applications, Pinholes and DMZ**.
4. Scroll down to the Edit Firewall settings for this computer pane.
5. Scroll down and click **Add a new user-defined application**.
6. Enter the following information:
   - **Application Profile Name**. A descriptive name for the application profile.
   - **Protocol**. Select TCP or UDP. If the application you are adding requires both, you can create a separate definition for each.
   - **Port (or Range)**. The port number or range of port numbers that the application uses. For example, some applications requires only one port to be opened (such as TCP port 500); others require that all TCP ports from 600 to 1000 be opened. If only one port is required, enter the port number in the From field.
   - **Protocol Timeout**. The amount of time in seconds that can pass before the application times out. If the field is blank, the gateway uses the default values (86400 seconds for the TCP protocol and 600 seconds for the UDP protocol).
   - **Map to Host Port**. A value that maps the port range you established in the Port field to the local computer. For example, if you set the value to 4000 and the port range being opened is 100 to 108, the forwarded data to the first value in the range will be sent to 4000. Subsequent ports will be mapped accordingly; 101 will be sent to 4001, 102 will be sent to 4002, and so on.
   - **Application Type**. Select the application type. If you do not know the application type, leave the field blank.
7. Click Add to List.

Allowing all applications (DMZplus)

DMZplus is a special firewall mode that is used for hosting applications. When in the DMZplus mode, the designated computer:

- Appears as if it is directly connected to the Internet.
- Has all unassigned TCP and UDP ports opened and pointed to it.
- Can receive unsolicited network traffic from the Internet.

Use DMZplus mode with caution. A computer in DMZplus mode is less secure because all available ports are open and all incoming Internet traffic is directed to this computer.

1. Open the gateway home page at http://192.168.1.254.
2. Click the **Settings** tab, then click the **Firewall** tab.
3. Click **Applications, Pinholes and DMZ**.
4. Select the computer that you want to put in DMZplus mode.

   If the computer you want to select is unlisted because it is powered off and the Hide inactive devices option is enabled, you can select it if it is on the same network and you know its IP address. Enter the IP address and click **Choose**.
5. Select **Allow all applications (DMZplus mode)**.
6. Click **Save**.
7. Confirm that the computer you selected is configured for DHCP. If it is not, configure it for DHCP. See “Configuring DHCP” on page 20.
8. Restart the computer. When the computer restarts, it receives a special IP address from the gateway and all unassigned TCP and UDP ports are forwarded to it.

To stop DMZplus mode on a particular computer, select it and then select **Maximum protection**.

Troubleshooting 4

This section provides information about common gateway installation issues. If an issue has more than one potential cause, the most common cause is listed first.

Connection issues

Use the information in this section to identify and resolve issues related to connectivity.

The Power light is not on

- The power cable may be loose or disconnected. Check the power cable to ensure that the cable is securely connected. If the power cable is plugged in to a power strip or switched outlet, ensure that it is on. Ensure that you are using the power supply that came with the gateway.
- The power supply may be faulty. Verify that the light on the power supply is green.
- The AC outlet may be faulty. Try plugging the gateway in to a known good outlet.

The Power light blinks immediately after the device starts, and then turns steady green

- The Power light blinks during POST (Power on self-test). This is normal behavior.

The Power light is red

- The POST (Power on self-test) may have failed. Press the Reset button and hold it for 10 seconds to reset the gateway.

The Broadband light blinks

- The Ethernet or DSL cable may be loose or disconnected. Check the connections to ensure that the cable is securely connected.
- The DSL connection may not be established. Press the Reset button and hold it for 10 seconds to reset the gateway. If resetting the gateway does not fix the problem, contact your service provider.

The Broadband light blinks green for a long time, then turns red

- The gateway may have failed to synchronize with the service provider network. Check the connections to ensure that the cable is securely connected.
- Your Internet service may not be activated. Contact your service provider.

The Service light blinks

- Your Internet service may not be activated. Contact your service provider.

The Service light is red

- The user name and password may have been entered incorrectly. Verify the user name and password on the gateway configuration page, and try again.
- Your Internet service may not be activated. Contact your service provider.

The Ethernet light is not on

- The Ethernet cable may be loose or disconnected. Check the connections to ensure that the cable is securely connected.

The Wireless light is not on

- No devices on your home network are currently connected to the gateway over the wireless connection.
- Ensure that the wireless feature is enabled. For more information, go to the gateway configuration page at http://192.168.1.254

The Internet is not accessible but the gateway configuration page is accessible

- The Ethernet or DSL cable may be loose or disconnected. Check the connections to ensure that the cable is securely connected.

LAN issues

Use the information in this section to identify and resolve issues related to the home network.

Can’t connect to the gateway through the Ethernet port

- The Ethernet cable may be loose or disconnected. Check the connections to ensure that the cable is securely connected. The **Ethernet** light blinks green when there is a working link to a device.

A wireless device cannot get an IP address

- The device may not be set up with the appropriate security type or security key. Ensure that the wireless device is using the appropriate credentials.
- The wireless device and the gateway may be using different wireless modes, such as 802.11b, 802.11g, 802.11n, or 802.11ac. Ensure that the wireless device and the gateway are using compatible modes.

The wireless signal is weak

- The wireless device may be out of range. Ensure that the wireless device is within the range of the gateway.

I cannot set a custom encryption key on the gateway user interface

- The custom encryption key may not conform with the security mode, key length, key type, or value type. Configure the custom encryption key so that it conforms to the security mode, key length, key type, or value type.

Regulatory Information A

Declaration of conformity

The following sections describe regulatory compliance by region.

FCC/Industry Canada compliance

This device has been tested and certified as compliant with the regulations and guidelines set forth in the Federal Communication commission - FCC part 15, FCC part 68 and Industry Canada - ICES003 and RSS-210 Radio and telecommunication regulatory requirements.

Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada. Cet appareil numérique de la classe [*] est conforme à la norme NMB-003 du Canada.

Manufacturer: Pace Americas
Model(s): 5268ac

Part 15 of FCC rules / IC RSS-210 - RSS GEN

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux normes CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Users should be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5470-5725 MHz and that these radars could cause interference and/or damage to the LE-LAN device.

Les utilisateurs doivent être avisés que les radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars peuvent causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

The device for operation in the band 5150-5250MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential for radio interference to other users, the antenna type and its maximum gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate this equipment.

TIA 968 (Part 68 of FCC rules)/IC CS-03

This equipment complies with the Telecommunication Industry Association TIA-968 (FCC part 68) and Industry Canada CS-03 Telecommunication requirements. On the product is a label that contains, among other information, the IC and FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information may be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the device not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0)

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum RENs for the calling area.

This product cannot be used on telephone-company-provided coin service. Connection to Party Line Service is subject to state tariffs.

An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications to maintain uninterrupted service. If trouble is experienced with this equipment, please contact Pace Americas, or your local Pace Americas distributor or service center in the U.S.A. for repair and/or warrant information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove this equipment from the network until the problem is resolved. No repairs can be done by a customer on this equipment. It is recommended that the customer install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damage to the equipment caused by local lightning strikes and other electrical surges.

MPE/SAR/RF exposure information

This device was verified for RF exposure and found to comply with Council Recommendation 1999/519/EC and FCC OET-65 RF exposure requirements. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

WARNING: While this device is in operation, a separation distance of at least 20 cm (8 inches) must be maintained between the radiating antenna inside the EUT and the bodies of all persons exposed to the transmitter in order to meet the FCC RF exposure guidelines. Making changes to the antenna or the device is not permitted. Doing so may result in the installed system exceeding RF exposure requirements. This device must not be co-located or operated in conjunction with any other antenna or radio transmitter.

Cet appareil répond aux directives d'exposition RF 1999/519/EC et FCC OET-65 sur la limitation d'exposition du public général aux champs électromagnétiques.

MISE AN GARDE: Pour satisfaire aux exigences de la FCC et IC concernant l'exposition aux radiofréquences, une séparation de 20 cm ou plus doit être maintenue entre cet appareil et des personnes lors de fonctionnement du dispositif. Pour assurer la conformité, des opérations au plus près que cette distance n'est pas recommandée. L'antenne utilisée pour cet émetteur ne doit pas être co-localisée ou fonctionner conjointement avec une autre antenne ou transmetteur.

Safety information

The following sections describe the safety guidelines for this product.

AC adapter

This product is intended to be supplied with a listed Pace Direct Plug-In AC/DC power adapter marked Class 2 or LPS and rated 12V 3A for all 5233N-xxx models.

The AC/DC power adapter supplied with this product is designed to ensure your personal safety and to be compatible with this equipment. Use only the power adapter that was provided with the gateway.

Please follow these guidelines:

- Do not use the adapter in a high moisture environment. Never touch the adapter when your hands or feet are wet.
- Allow adequate ventilation around the adapter. Avoid locations with restricted airflow.
- Connect the adapter to a proper power source. The voltage and grounding requirements are found on the product case and/or packaging.
- Do not use the adapter if the cord becomes damaged.
- Do not attempt to service the adapter. There are no serviceable parts inside. Replace the unit if it is damaged or exposed to excess moisture.

Adaptateur secteur

Cet appareil est destiné à être alimenté par une source d’alimentation directe fournie par Pace ou 2Wire, de « Classe 2 » ou marquée « LPS », et avec un courant de sortie de 12 V DC, 3 A pour tous les modèles 51xxNV-xxx et 51xxN-xxx.

Le bloc d’alimentation secteur fourni avec ce produit a été conçu pour garantir votre sécurité et être compatible avec cet appareil.

Veuillez suivre les consignes suivantes:

- N’utilisez pas l’adaptateur secteur dans un environnement hautement humide. Ne touchez jamais l’adaptateur secteur si vos pieds ou mains sont humides.
- Laissez une ventilation adéquate autour de l’adaptateur secteur. Evitez les endroits où la circulation de l’air est insuffisante.
- Branchez l’adaptateur secteur sur une prise respectant les spécifications sur la tension et la mise à la terre se trouvant sur la coque et/ou l’emballage du produit.
- N’utilisez jamais l’adaptateur secteur si le cordon d’alimentation est endommagé.
- N’essayez pas de réparer vous-même cet adaptateur. Il n’y a aucune pièce réparable à l’intérieur. Remplacez l’adaptateur s’il est endommagé ou a été soumis à une humidité excessive.

Telecommunication cord

Caution: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Cordon téléphonique

Attention: Afin de réduire le risque d’incendie, n’utilisez qu’un cordon téléphonique de calibre 26 AWG ou supérieur listé UL ou certifié CSA.

Internal telephone ports (VoIP)

Telecommunication equipment connected to this port (e.g., via “Phone Lines 1 & 2” port) should be UL Listed and the connections shall be made in accordance with Article 800 of the NEC.

Port téléphonique (VoIP)

Tout équipement de télécommunication téléphonique connecté à ce port doit être listé UL et les branchements doivent être fait conformément aux dispositions de l’Article 800 du Code national de l’électricité (NEC).

Repairs

Do not, under any circumstances, attempt any service, adjustments, or repairs on this equipment. Instead, contact your local Pace Americas distributor or service provider for assistance. Failure to comply may void the product warranty.

Location - electrical considerations

CAUTION: Due to risk of electrical shock or damage, do not use this product near water, including a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool. Also, avoid using this product during electrical storms. Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, neon signs, high-frequency or magnetic security devices, or electric motors).

Emplacement – Considération électriques

AVERTISSEMENT: Pour éviter un risque de choc électrique, n'utilisez pas cet appareil à proximité d'une source d'eau, par exemple près d'une baignoire, un lavabo, une machine à laver, dans un garage humide ou près d'une piscine. Evitez aussi d'utiliser cet appareil durant un orage. Evitez de brancher cet appareil à proximité d'appareils électriques pouvant causer de large fluctuations de tension ou émettant du bruit électrique (tel que climatiseurs, enseignes au néon, dispositifs de sécurité magnétique ou de haute-fréquence, ou moteurs électriques).

Location - environmental considerations

Do not plug the AC/DC power adapter into an outdoor outlet or operate the residential gateway outdoors. It is not waterproof or dustproof, and is for indoor use only. Any damage to the unit from exposure to rain or dust may void your warranty.

Do not use the residential gateway where there is high heat, dust, humidity, moisture, or caustic chemicals or oils. Keep the gateway away from direct sunlight and anything that radiates heat, such as a stove or a motor.