NETGEAR® LTE Gateway LG6100D

User Guide

Table of Contents

Get Started

The following topics give you all the information you need to set up your gateway and Sprint service the first time.

Package Contents

Your package includes several items.

- NETGEAR 4G LTE Gateway 6100D

- Power adapter

- Micro-SIM (pre-installed)

- Ethernet cable

- Get Started poster

Your Gateway

The following illustrations show your gateway's LEDs, buttons, and connectors.

Front View
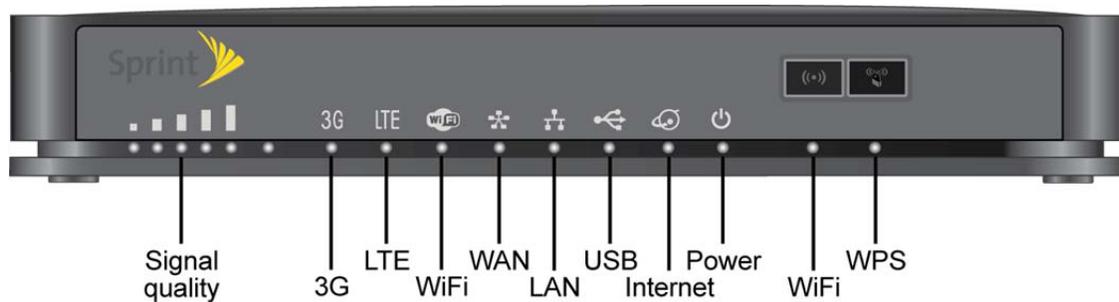
Back View
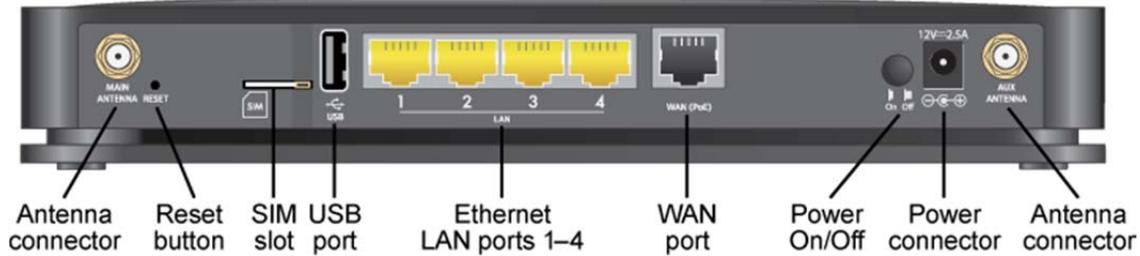
Care and Maintenance

As with any electronic device, you should handle the gateway with care to ensure reliable operation. Follow these guidelines in using and storing your device.

- Protect your device from liquids, dust, and excessive heat.

- Do not apply adhesive labels to your device. They may cause your device to overheat and may alter the antenna's performance.

System Requirements

The following items are required to use your NETGEAR 4G LTE Gateway 6100D.

- One or more computers that support Wi-Fi (802.11b/g/n or 11ac)

- Web browser (required if you'll be using the browser interface to view status and to configure settings). The following browsers are supported:

  - Internet Explorer (version 8 and above)

  - Firefox (version 3.6.24 and above)

  - Chrome (version 30 and above)

If you'll be connecting to your gateway through Ethernet:

  - Computer with an available Ethernet port

Set Up Your Gateway

The following topics describe how to set up and start using your gateway.

Attach the Antennas

The gateway comes with two external antennas that are interchangeable.

1. Attach the antennas to the gateway.

2. Adjust the antennas so that they are vertical.

Place Your Gateway

Place your gateway in a location with a good 3G or LTE signal.

1. Place your gateway in a location with good 3G or 4G coverage, such as near a window.

Note: When the gateway is powered on, you can use the Signal Quality LED to position the gateway in the location with the best signal strength.

2. Also, for best results, place your gateway:

   ▪ Near the center of the area where your computers and other devices operate, and preferably within line of sight to your Wi-Fi devices.

- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.

- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the gateway and your other devices to a minimum.

- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, computers, the base of a cordless phone, or a 2.4 GHz cordless phone.

- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Start Your Gateway for the First Time

Learn how to start your gateway for the first time.

The gateway is designed to activate automatically the first time that it is turned on using 'hands-free activation'. Typically, the activation process will be seamless, not requiring any action on your part.

To start your gateway:

1. Connect the power adapter to the gateway and plug the power adapter into an electrical outlet.

2. Make sure that the Power On/Off button on the rear panel of the gateway is pressed in.

   - The **Power** and **Wi-Fi** LEDs light.

   - The gateway automatically connects to a 3G or LTE network, and the **3G** LED or the **LTE** LED lights.

   - The **Internet** LED lights to show that you have Internet access.

If your account did not activate for some reason, connect to the gateway network and use a Web browser to log in to the gateway. Alerts on the home page allow you to try the activation again. You must activate your account before you can use Sprint data services.

Connect to Your Gateway's Network

You can connect with Wi-Fi or you can use an Ethernet cable for a wired connection to an Ethernet LAN port.

Tip: The Wi-Fi network name and password are on the label of the gateway.

Tip: Alternatively, you can use WPS to connect your computer or device to the gateway, if your computer or device supports WPS. (See Connecting Through WPS.)

To find and select a Wi-Fi network, then connect with Wi-Fi:

1. Do one of the following, depending on your operating system.

   - Windows 7: Right-click the Wi-Fi icon in the system tray.

   - Windows Vista: Click **Control Panel > Network and Internet > Network and Sharing Center > Connect to a network**.

   - Windows XP: Click **Control Panel > Network Connections > Wireless Network Connections > View available wireless networks**.

   - Mac: Click the AirPort icon (in the upper right corner of your screen).

   - Linux: Please see the user documentation of the Linux distribution.

   - Other operating systems: Please see the user documentation for your operating system or computer.

2. Select the Wi-Fi network for the gateway and connect to it. (If prompted for a network key/security key/password, enter the Wi-Fi password on the gateway label.)

To use WPS to connect with Wi-Fi:

3. Check the WPS instructions that came with your computer or wireless device.

4. Press the WPS button on the gateway.

   - For 2 minutes, the gateway tries to detect a computer or wireless device that is using WPS to connect to its Wi-Fi network.

5. On your computer or wireless device, press its WPS button or follow its WPS instructions.

   - Your computer or wireless device connects to the Wi-Fi network.

To connect with Ethernet:

A yellow Ethernet cable comes in the package with your gateway.

1. Connect an Ethernet cable (included in the package) to one of the yellow Ethernet LAN ports on the rear panel of the gateway.

3. Connect the other end of the Ethernet cable to an Ethernet port on your computer.

The **Ethernet LAN** LED on the gateway lights.

Your computer connects to the gateway's local area network (LAN). A message might display on your computer screen to notify you that an Ethernet cable is connected.

Get Help

Learn where you can get more information or assistance.

Visiting the Sprint Website

Sign on to sprint.com to get up-to-date information on Sprint services and options.

- Review coverage maps.

- Access your account information.

- Add additional options to your service plan.

- Purchase accessories.

- Check out frequently asked questions.

- And more.

Contacting Sprint Customer Service

You can reach Sprint Customer Service online or by calling toll-free.

- Log in to your account at sprint.com.

- Call us toll-free at **1-888-788-4727** (business use) or **1-888-211-4727** (personal use).

Gateway Basics

Learn about the buttons, connectors, and other components of your gateway.

Your gateway provides a simple way to use your Internet connection (3G or LTE) with any Wi-Fi-enabled device, and to share your Internet connection with friends and family.

Components of Your Gateway

Your gateway consists of several main components.

- **Main and Guest Wi-Fi networks**: The Wi-Fi networks (access points) connect your computers and other Wi-Fi-enabled devices to the gateway.

- **Main Wi-Fi dual-band**: The gateway has two Main Wi-Fi networks, so you can connect with 2.4 GHz or 5 GHz Wi-Fi. To connect with 5 GHz, your computer or Wi-Fi-enabled device must support 5 GHz.

- **Modem**: The modem connects your gateway to the Internet via the best available network (customizable):

  - LTE – Newer technology, faster speeds compared with 3G

  - 3G – CDMA technology, more widely available compared with LTE

- **Routing hardware**: The routing hardware handles traffic between the modem, the Wi-Fi access point, and the Wi-Fi network.

- **USB port**: You can connect a USB drive and share it.

3G and LTE Networks

These wireless networks connect you to the Internet.

Depending on your coverage area, you may have:

- Only LTE coverage

- Only 3G coverage

- A combination of these networks

The gateway automatically connects to the fastest network that is available to you. If you have both 3G and LTE coverage and your connection happens to get disrupted, your gateway can automatically switch to the other network. (For more information, see Mobile Broadband Information and Settings.)

Your gateway is designed to always connect to an available network if possible. If your gateway is not connected (dropped signal, roaming not supported, etc.) the Signal Strength LED is off. The connection status can also be seen on your gateway's Network > Status Details Page.

Your gateway can be set to connect automatically to the best available network, or to connect to LTE or 3G networks only. See Setting the Allowed Network Mode.

Your gateway can also be set to allow roaming on Sprint networks, domestically, and internationally. See Setting the Roaming Mode.

Power Button

Use the Power button to turn your gateway on and off.

To turn your gateway on:

1. Make sure that power adapter for your gateway is plugged in to an electrical outlet.

2. Press the **Power On/Off** button so that it is in the on position.

Note: The LEDs on the gateway light unless you logged in to the gateway and turned off the LEDs from the Device page.

To turn your gateway off:

- ■ Press the **Power On/Off** button so that it is in the off position.

Note: The LEDs on the gateway turn off.

LEDs

The LED status indicators show the gateway's Internet and network connections.

LED	Description
Signal Quality	**5 bars**: Excellent coverage. **4 bars**: Strong coverage. **3 bars**: Moderate coverage. **1 bar**: Poor coverage. **Off**: No coverage.
3G Connection	**Solid blue**: The gateway has a connection with the 3G network. **Off**: The gateway does not have a 3G connection.
LTE Connection	**Solid blue**: The gateway has a connection with the 4G LTE network. **Off**: The gateway does not have a 4G connection.
Wi-Fi	**Solid green**: The 2.4 GHz wireless radio is on. **Solid purple**: The 5 GHz wireless radio is on. **Solid blue**: Both the 2.5 GHz and the 5 GHz wireless radios are on. **Off**: The wireless radios are off.
Ethernet WAN	**Solid blue**: The Ethernet WAN port is connected to a device and is ready. **Off**: The gateway does not detect a link on this port.
Ethernet LAN	**Solid blue**: One or more local Ethernet ports 1-4 have detected wired links. **Off**: The gateway does not detect links on these ports.
USB	**Solid blue**: The gateway has accepted the USB device and the USB device is ready.

	Off: No USB device is connected.
Internet	**Solid blue**: The Internet connection is ready.
	Solid amber: Network error.
	Slow blinking amber: The gateway failed to cut over from an Internet WAN connection to a mobile broadband connection.
	Off: No Internet connection.
Power	**Solid green**: The gateway is ready.
	Slow blinking green: The gateway is powering up.
	Solid red: System failure.
	Slow blinking red: Thermal cut off alarm.
	Off: No power is supplied to the gateway.
Wi-Fi On/Off	**Solid blue**: The wireless radios are on.
	Off: The wireless radios are off.
WPS	**Solid blue**: WPS security is enabled.
	Blinking blue: Someone is using WPS to join the gateway's Wi-Fi network.
	Off: WPS is not in use.
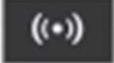
Micro-SIM

Your gateway comes with a pre-installed micro-SIM that gives you access to the Sprint network.

Launch Your Mobile Network Connection

After your gateway powers on and boots up, a connection to the best available network (3G, 4G, or LTE) is launched automatically.

Your gateway remains connected at all times, unless:

- You are out of signal range or the signal is blocked.

- You are in a roaming area and you have chosen not to allow roaming.

Note: Even though your gateway is connected, you are only billed when data is sent or received. See If the Connection is "Always On," Am I Always Being Billed?

Web Browser Interface

When you connect to the gateway network (either with Wi-Fi or with an Ethernet cable), you can use a Web browser to log in to your gateway to view or change its settings.

Log In to Your Gateway

Tip: If you want to change your gateway's Wi-Fi settings, use a wired Ethernet connection to avoid being disconnected when the new Wi-Fi settings take effect.

To log in to your gateway:

1. On a computer or wireless device that is connected to your gateway's network, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

   Note: If you're using the Google Chrome Web browser, after typing in the address bar, press the **Down Arrow** key and then press the **Enter** key. (If you don't press the **Down Arrow** first, a Google search starts and you are not prompted to log in to your gateway.)

4. If your Web browser displays an error message, see Cannot Display the Home Page.

Home Page

The home page is the entry page when you log in to the gateway.

You can:

- Activate your account if it did not automatically activate.

- View your data usage and status information for your data connection.

- Manage your mobile broadband network connection and Wi-Fi connections.

- View alert messages.

Item	Description
Home	Click to view the Home Page.
Devices	Click to view the Devices Page.
Wi-Fi	Click to view the Wi-Fi Page.
GPS	Click to view the GPS Page.
Settings	Click to view the Settings Page.
Connection Details	Mobile broadband connection information – See Mobile Broadband Information and Settings.
Devices Connected	List of devices connected to the gateway's Main or Guest Wi-Fi networks.
My Account Summary	Basic information about your Sprint data plan. For more details, click **My Sprint** to connect to your account at mysprint.sprint.com/mysprint.
Twitter[®]	Click to view the AirCard Twitter feed in a new browser window or tab. (Your

	device must be connected to the network for this option to work.)
Facebook®	Click to view the AirCard Facebook page in a new browser window or tab. (Your device must be connected to the network for this option to work.)
Feedback	Click to send NETGEAR your comments on your gateway. See Feedback Page. (Your device must be connected to the network for this option to work.)
International Information	Click to view Sprint's International Coverage Areas search feature in a new browser window or tab. (Your device must be connected to the network for this option to work.)
Important Information	Click to read important safety information about the gateway.
Alerts	Alerts remain until issue is resolved.
Data Usage Session	Estimated data usage for current session.
Data Usage of This Month	Estimated data usage for current billing period.

Alerts

Alerts notify you about situations that require your attention and suggest the actions you need to take to resolve them.

The following information is displayed for each alert.

Item	Description
Alert title	A short description of the issue to be addressed.
Description	The alert message and, if appropriate, links or buttons to take action on the alert. (For example, the "Update now" link in the second alert shown above would take you to the Software Update screen.)

The alerts disappear only when the issues they describe are resolved. See Alerts for a list of alerts you may encounter and the corrective actions required.

Some of the alerts you may encounter include:

- Software Update Available

- Max Wi-Fi devices reached

- Mobile Broadband disconnected

- Wi-Fi is off

- Gateway is not activated

- SIM errors

- Roam Guard

Activate Your Account from the Home Page

Until your account is activated, you cannot use Sprint data services.

To activate your account:

1. On the home screen, go through the alerts until you see the **Hotspot not activated** alert.

2. Click **Retry Activation**.

3. Follow any instructions that may appear.

Data Usage

Data usage estimates are shown in the Data Usage section of the home page.

Data Usage		
Session:		
Data Used	Elapsed Time	
0.12 MB	0 day 00 hr 13 min 39 sec	Reset
Usage Of This Month :		
		Days Left
		18
Total used in this month : 0.12 MB		
Used This Month:		

	Sent	Received	Combined
4G	0.06MB	0.06MB	0.12MB
3G	0.00MB	0.00MB	0.00MB
Total	0.06MB	0.06MB	**0.12**MB

Displayed data usage is intended to help manage usage. The amounts shown are approximate and may vary.

Note: Data usage amounts are approximate and should not be used for billing purposes. For accurate data usage amounts, check with Sprint or click the My Sprint link in the My Account Summary section to view your account details.

The Data Usage section displays monthly billing period statistics and current session statistics.

Item	Description
Current billing cycle	
Usage of This Month	The amount of data sent and received during the billing period for each network type.
Reset button	Click to set the displayed monthly usage values to 0MB. **Important:** This does **not** reset the actual data usage for the billing cycle.
Session	
Used	Data amount used since your device connected to the network
Elapsed time	Length of time that your device has been connected to the network

My Account Summary

The My Account Summary section shows basic information about your plan, and includes a link to see more detailed information.

My Account Summary

My Data Plan: 3G/4G Demo Connection Plan

My Number: 9136536034

My Sprint

The following information is displayed.

Item	Description
My Data Plan	The type of Sprint data plan used on your gateway.
My Number	The telephone number linked to your data plan.
My Sprint	Click to connect to your account at mysprint.sprint.com/mysprint.

Connection Details

The Connection Details section shows details about your mobile broadband service and connection state, and lists the devices that are connected to the Main and Guest Wi-Fi networks.

The following information is displayed.

Item	Description
Signal strength and roaming status	The more bars, the stronger the signal. A triangle in the icon means your device is roaming. See Signal Information for details.
Network carrier name	Name of the available network. For example, "Sprint".
Network type	LTE or 3G
Send / Receive indicators	⬆⬇ Up (sending data) / Down (receiving data) This icon appears when you are connected to the mobile network.
Roaming message	Indicates whether your device is roaming on a Sprint network, domestically, or internationally.
Connect / Disconnect button	Click this button to connect or disconnect your device from the mobile network.
Devices	**Wi-Fi 2.4 GHz**: A list of devices currently connected to the Main Wi-Fi 2.4

Connected	GHz network.
	Wi-Fi 5 GHz: A list of devices currently connected to the Main Wi-Fi 5 GHz network
	Guest Wi-Fi: A list of devices currently connected to the Guest Wi-Fi network.
	You can click any of the device names to view their details, or to block them from using your network. See Displaying and Blocking Currently Connected Devices (Block List).

Your Network Connections

Find out how to launch, share, and end your Internet network connection.

Launch Your Mobile Network Connection

After your gateway powers on and boots up, a connection to the best available network is launched automatically.

Your gateway remains connected at all times, unless:

● You are out of signal range or the signal is blocked.

● You are in a roaming area and you have chosen not to allow roaming.

Note: Even though your gateway is connected, you are only billed when data is sent or received. See If the Connection is "Always On," Am I Always Being Billed?

Set up a Guest Wi-Fi Network

You can create a separate Guest Wi-Fi network that you can share with temporary users.

Computers and wireless devices on the Guest Wi-Fi network:

● Cannot access devices that are on the Main Wi-Fi network (such as printers or other computers)

● Cannot log in to the gateway to change its settings

Turn the Guest Wi-Fi Network On

You can turn on the Guest Wi-Fi network on the gateway's Wi-Fi page.

To turn the guest Wi-Fi network on:

4. On a computer or wireless device that is connected to your gateway, launch a Web browser.

5. In the address or URL field of your browser, type **http://myrouter**.

6. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

7. Click **Wi-Fi**.

8. In the Guest Wi-Fi area, click **Turn On**.

Turn the Guest Wi-Fi Network Off

You can turn off the Guest Wi-Fi network on the gateway's Wi-Fi page.

To turn the guest Wi-Fi network off:

9. On a computer or wireless device that is connected to your gateway, launch a Web browser.

10. In the address or URL field of your browser, type **http://myrouter**.

11. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

12. Click **Wi-Fi**.

13. In the Guest Wi-Fi area, click **Turn Off**.

Share Your Wi-Fi Network

Your gateway provides two ways of sharing your network connection with other users.

- Users find and select the Main or Guest Wi-Fi network information.

- User connects to the Main or Guest Wi-Fi network using WPS.

Manually Enter the Wi-Fi Information

Users can connect to the network by manually entering the Wi-Fi information.

Share your network connection with others:

1. Provide the Main or Guest Wi-Fi network name and password to them.

2. Users must open their device's Wi-Fi network manager and connect to the Main or Guest Wi-Fi network using the password you provided. (See How Do I Connect to Wi-Fi?)

Connect Through WPS

Wi-Fi Protected Setup (WPS) provides a fast, simple, and secure way to connect WPS-enabled devices to your Wi-Fi network.

With WPS, you don't have to give the name (SSID) and Wi-Fi password of your Main or Guest network to other users. The WPS feature is available on certain cameras, printers, smartphones, and laptops. These devices have either a hardware button or a WPS-related option in the software. Please consult the user documentation of your device.

WPS is always available for the Main and Guest Wi-Fi networks as long as the Wi-Fi radio is on.

WPS is not available in the following situations:

- The Wi-Fi radio is off because someone pressed the Wi-Fi On/Off button on the gateway.

- The Wi-Fi security option is WPA Personal, WEP, or WEP-related (for example, "WEP 64 Bit Open"). (WPS is available if the Wi-Fi security option is WPA/WPA2 Personal.) (See Wi-Fi Security.)

- Broadcast network name is not enabled. (See Options Tab.)

- MAC Filter Mode is "White list (Allow only those in list)", but no computers have been added to the list. (See "Specifying Computers That Can Access the Network" in Allowing or Denying Computers Access to the Network (MAC Filter).)

If the maximum number of connected devices on the chosen network (Main or Guest) has already been met, an error message indicating that the maximum number of devices has been reached is displayed when you attempt WPS. Disconnect one of the connected devices and then retry.

You can use the WPS button on the gateway or you can log in to the gateway and use the **Wi-Fi > Connect** page.

Devices Page

The Devices page lets you see lists of devices that are connected to your Main and Guest Wi-Fi networks.

Note: These lists are also shown in the **Devices Connected** section on the left side of the page.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Devices**.
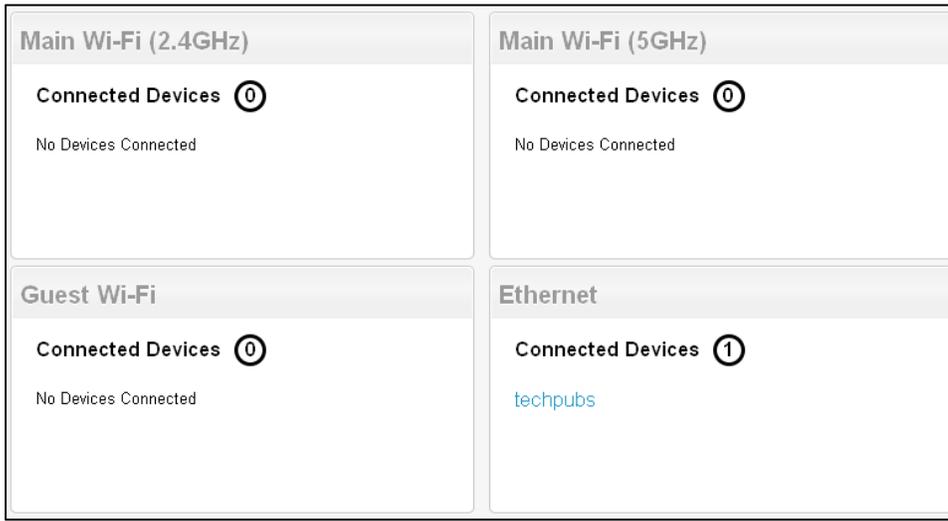
The following information is displayed.

Item	Description
Main Wi-Fi (2.4 GHz)	A list of devices currently connected to the Main Wi-Fi network in the 2.4 GHz band.
Main Wi-Fi (5 GHz)	A list of devices currently connected to the Main Wi-Fi network in the 5 GHz band.
Guest Wi-Fi	A list of devices currently connected to the Guest Wi-Fi network.
Ethernet	A list of devices currently connected to the device through an Ethernet connection to an Ethernet LAN port.

You can click any of the device names to view detailed information, and to block them from using your network. See Displaying and Blocking Currently Connected Devices (Block List).

Wi-Fi Connect Page

From the Wi-Fi page, you can configure the Wi-Fi network, including Wi-Fi security.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi**.
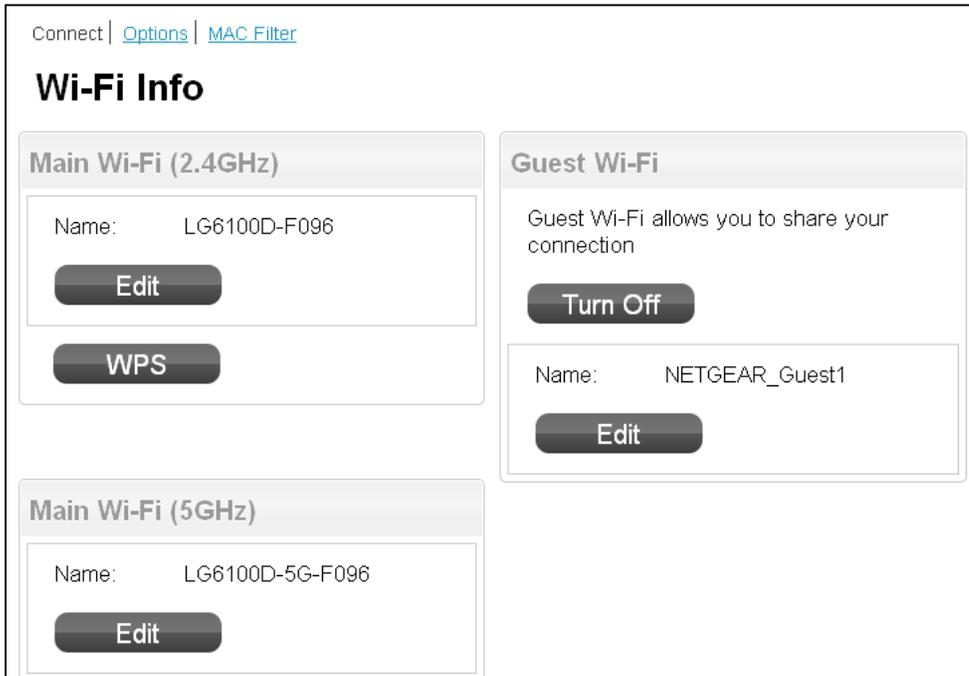
You can configure access to your Main and Guest Wi-Fi networks.

You can:

- Edit the Main or Guest Wi-Fi names and passwords. See Change Wi-Fi Network Names and Passwords.

- Turn the Guest Wi-Fi network on or off. See Setting up a Guest Wi-Fi Network.

- Connect devices using WPS. See Connecting Through WPS.

The following information is displayed.

Item	Description
Main Wi-Fi (2.4 GHz)	
Name	This is the name that identifies your Main Wi-Fi network and is visible to other Wi-Fi-enabled devices. See Change Wi-Fi Network Names and Passwords.
WPS	Connect a device to the Main Wi-Fi network using WPS. See Connecting Through WPS.
Main Wi-Fi (5 GHz)	
Name	This is the name that identifies your Main Wi-Fi network and is visible to other Wi-Fi-enabled devices. See Change Wi-Fi Network Names and Passwords.
WPS	Connect a device to the Main Wi-Fi network using WPS. See Connecting Through WPS.

Guest Wi-Fi	
Turn Off / **Turn On**	Click this button to turn the Guest Wi-Fi network on or off. **Note:** The rest of the Guest Wi-Fi fields / buttons appear only when the Guest Wi-Fi network is on.
Name	This is the name that identifies your Guest Wi-Fi network and is visible to other Wi-Fi-enabled devices. See Change Wi-Fi Network Names and Passwords.

Wi-Fi Options Page

From the Wi-Fi Options page, you can configure your Wi-Fi network's connection settings and security, and additional Wi-Fi options.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > Options**.

You can:

- Edit the Main or Guest Wi-Fi names and passwords. See Change Wi-Fi Network Names and Passwords.

- Configure your Wi-Fi network's connection parameters and security, and additional Wi-Fi options.

- Specify the maximum number of devices that can connect to the WiFi network.

Note: For some of these Wi-Fi settings, if you change them, all connected devices will be disconnected and have to reconnect after the settings are saved.

The following information is displayed.

Item	Description
Main Wi-Fi	
Network Name	This is the name that identifies your Main Wi-Fi network and is visible to other Wi-Fi-enabled devices. (See Change Wi-Fi Network Names and Passwords.)
Guest Wi-Fi	
Network name	This is the name that identifies your Guest Wi-Fi network and is visible to other Wi-Fi-enabled devices. (See Change Wi-Fi Network Names and Passwords.)
Wi-Fi Options	
Wi-Fi Range	Short Medium Long
Connection	
Connection Rate	This setting determines the type of Wi-Fi devices that can connect to your network. For the Main and Guest 2.4 GHz networks, the default connection is **Up to 300 Mbps**. The other choices are **Up to 130 Mbps** and **Up to 54 Mbps**. For the 5 GHz network, the default connection rate is **Up to 300 Mbps**. The other choices are **Up to 400** Mbps and **Up to 800 Mbps**.
Wi-Fi Channel	This is the active channel of the Wi-Fi access point. If your network is having performance issues (possibly caused by other Wi-Fi networks in the vicinity using the same channel), try a different Wi-Fi channel. See Wi-Fi Channel.
RTS Threshold	This setting specifies the smallest packet size, in bytes, for which RTS/CTS (Request to Send/Clear to Send) handshaking is used. The recommended value is 2347. Change this value only if you're experiencing inconsistent data flow. Make only minor changes to this value.

Fragmentation Threshold	This setting specifies the largest allowable size, in bytes, for a packet. If the packet is larger than this, it is fragmented into multiple packet before it is transmitted. To prevent poor network performance, it's recommended to keep this value as large as possible (up to 2346).
Security	
Broadcast Network Name	If broadcast is enabled (**Yes**), the wireless network is displayed in the list of Wi-Fi networks available in the local area. For increased security, set this field to **No**. You will need to give the Wi-Fi network name (Main or Guest) to the people who will be accessing your network, and WPS will not be available.
Encryption	The type of security used by the Main Wi-Fi network. See Wi-Fi Security.
Guest Encryption	The type of security used by the Guest Wi-Fi network. See Wi-Fi Security.

MAC Filter

MAC (Media Access Control) filtering can prevent unauthorized wireless devices from connecting to your network.

The MAC filter is used to grant ("white list") or block ("black list") wireless devices access to the Wi-Fi and mobile broadband (3G or LTE) networks. Access is based on the MAC address of each wireless device.

MAC filtering increases security of your network. You can give access to your network, based on the MAC address of the wireless devices. This makes it harder for a hacker to use a MAC address to access your network.

To set up MAC filtering or turn it off:

5. On a computer or wireless device that is connected to your gateway, launch a Web browser.

6. In the address or URL field of your browser, type **http://myrouter**.

7. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

8. Click **Wi-Fi > MAC Filter**.
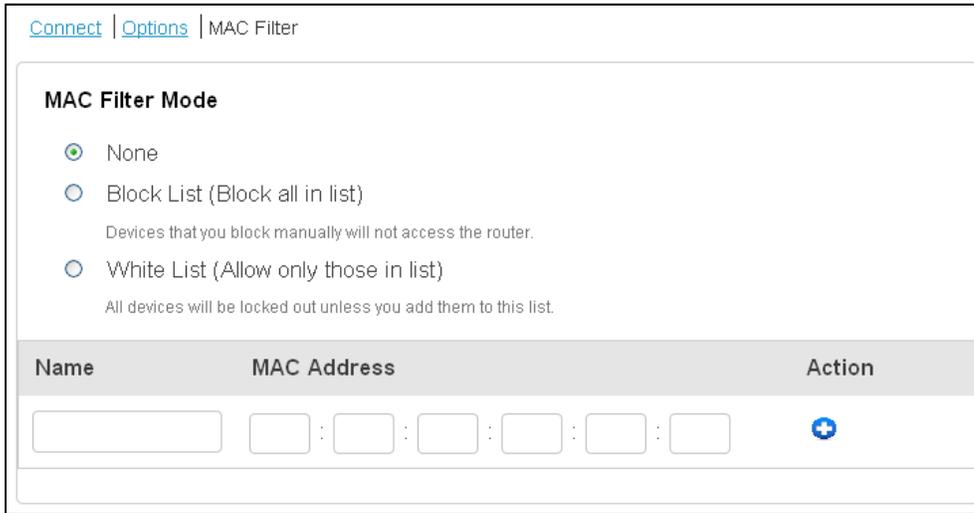
You can:

● Turn MAC filtering off ("None") or on ("Block List" or "White List").

● Add or remove a device from the list. (See "Specifying Computers That Can Access the Network" and "Specifying Computers That Are Not Allowed to Access the Network" in Allowing or Denying Computers Access to the Network (MAC Filter)).

The following information is displayed.

Item	Description
MAC Filter Mode	● **None** – Any device can connect to the Wi-Fi networks. ● **Black List** – The listed devices will not be able to connect to the Wi-Fi networks. ● **White List** – Only the listed devices will be allowed to connect to the Wi-Fi networks.
Black List or **White List**	
Name	A description of the device (the owner's name, the device's purpose, etc.)
MAC Address	The device's MAC address.

Wi-Fi security

Learn about the Wi-Fi security options available to you.

By default Wi-Fi security is enabled for your device and its Wi-Fi networks.

Note: All devices used with the gateway must support the selected security type.

Note: WPS is available only if you select either a WPA2 Personal option (including WPA/WPA2 Personal) or no security (not recommended). (See Connecting Through WPS.)

Note: WEP is available only for the guest network.

You can change the security used for Wi-Fi:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > Options**.

5. In the list beside **Encryption** (for Main Wi-Fi) or **Guest Encryption** (for Guest Wi-Fi) select one of the following options. Note that not all options may be available, depending on the **Connection Rate**.

   - **None**: No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

   - **WEP 64 Bit – Open**: This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

     Open WEP uses the key for encryption, but not for authentication.

   - **WEP 64 Bit – Shared**: This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

     Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

   - **WEP 128 Bit – Open**: This option provides security, but it's relatively weak (but stronger than **WEP 64 Bit – Open**). This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

     Open WEP uses the key for encryption, but not for authentication.

- **WEP 128 Bit – Shared**: This option provides security, but it's relatively weak (but stronger than **WEP 64 Bit – Shared**). This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

- **WPA PSK TKIP**: This is a strong security standard that is supported by most Wi-Fi devices.

- **WPA2 PSK AES**: This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WPA2 PSK TKIP**: This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WPA/WPA2 Enterprise** (recommended setting if any of your devices are more than two years old): Wi-Fi devices that use either WPA or WPA2 can connect to the NETGEAR 6100D. Supported by most Wi-Fi devices.

6. Click **Submit**.

The option you select determines the Wi-Fi security used and also the maximum length of the Wi-Fi password.

Change Wi-Fi Network Names and Passwords

The Main and Guest Wi-Fi network names identify your Wi-Fi networks and are visible to other Wi-Fi-enabled devices.

You can change the names and passwords for your Main and Guest Wi-Fi networks on the gateway's **Wi-Fi > Options** page.

For optimal security, you should make your Wi-Fi network names and passwords unique, and change them on a regular basis.

Note: If you change either of the Wi-Fi network names or passwords, all connected devices will be disconnected and will have to reconnect using the new values.

Note: For security reasons, it's recommended you disable SSID Broadcast. (See Options Section.)

To make your Wi-Fi passwords more secure:

- Use numbers and both uppercase and lowercase letters.

- Use special characters (for example, '@', '#', etc.).

Also, the password length depends on the Wi-Fi encryption type that you've selected. (See Wi-Fi Security.)

- None – No password is required.

- WEP 64 bit – Open: The password must be 5 ASCII characters.

- WEP 64 bit – Shared: The password must be 5 ASCII characters.

- WEP 128 bit – Open: The password must be 13 ASCII characters.

- WEP 128 bit – Shared: The password must be 13 ASCII characters.

- WPA-Personal TKIP: The password must be 8 to 63 ASCII characters.

- WPA-Personal TKIP/AES: The password must be 8 to 63 ASCII characters.

- WPA2-Personal TKIP/AES: The password must be 8 to 63 ASCII characters.

- WPA/WPA2 Personal: The password must be 8 to 63 ASCII characters.

To change the Wi-Fi network name and password:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > Options**

5. In the Main Wi-Fi and Guest Wi-Fi sections, change the **Network Name** and **Password** fields as desired. (The required lengths appear beneath the fields.)

6. Click **Submit**.

7. When prompted, click **Submit** again. (All devices that were connected will have to reconnect with the new settings.)

Enable or Disable the Block List

You can enable your gateway's block list on the gateway's Wi-Fi MAC Filter page. This lets you identify devices that should not be allowed to access your Wi-Fi networks.

To enable or disable the Wi-Fi block list (MAC filtering):

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > MAC Filter**.

5. Beside **MAC Filter Mode**, select **Black List** to block devices, or select **White List** to prevent devices from being blocked.

6. Click **Submit**.

Display and Block Currently Connected Devices (Block List)

To detect a potential intruder, you may want to display a list of the Wi-Fi-enabled devices that are currently connected to your gateway. You can view this list the gateway's home page.

To stop a device from connecting to your network, you can add it to your gateway's block list. The blocked device will not be able to connect again until you choose to unblock it. (See View and Unblock Devices (Block List).)

Note: You have to enable the block list before you can block devices from using your Wi-Fi networks. (See Enable / Disable the Block List.)

To manage the block list:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

   The **Devices Connected** section of the home page shows a list of the devices connected to your Main and Guest Wi-Fi networks.

4. To block a listed device, click its device name. The device's IP address and MAC address display.

5. Click **Block Device**.

6. Click **Block Device** again.

View and Unblock Devices (Block List)

You can view a list of devices that you have blocked (see Displaying and Blocking Currently Connected Devices (Block List)) from connecting to your gateway on your gateway's **Wi-Fi MAC Filter** page.

To allow any of these devices to connect to the network again, you can remove them from your device's block list.

To view and unblock devices on the block list:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > MAC Filter**. A list of the devices blocked from using your Wi-Fi networks appears.

5. Click the ⊗ beside the device you want to unblock. The device is removed from the list immediately.

Allow or Deny Computers Access to the Network (MAC Filter)

MAC (Media Access Control) filtering can prevent unauthorized wireless devices from connecting to your network.

The MAC filter is used to grant ("white list") or block ("black list") wireless devices access to the Main and Guest Wi-Fi networks. Access is based on the MAC address of each wireless device.

In the MAC Filter page (Wi-Fi > Mac Filter), you can choose one of three modes:

- **None** – All computers are allowed to access the network.

- **Black list** – All computers are allowed to access the network, unless they're in this list.

- **White list** – Only computers that are in this list are allowed to access the network.

Regardless of the mode, a user must provide the correct Wi-Fi password to access the network.

To specify computers that can access the network:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > MAC Filter**.

5. Beside MAC Filter Mode, select **White list**.

4. In the empty **Name** field, enter a name for the device. For example, "Amy's PC".

5. In the empty **MAC Address** field, enter the MAC address of the device you're adding to the list. (If you don't know this address, see Finding the MAC Address.)

   Click the ⊕ beside the row.

6. Repeat steps 4 and 5 for each computer for which you want to allow access.

IMPORTANT: Make sure you add the computer you are using, or else you will not be able to access the network after your device resets.

7. Click **Submit**.

To specify computers that are not allowed to access the network:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > MAC Filter**.

5. Beside MAC Filter Mode, select **Black list**.

6. Determine and block an undesired user of your network:

● In the Devices Connected section, if you see a device you don't recognize, you can click its name and compare its MAC address to the MAC address of each of the devices on your network.

   To determine the MAC address of each device you have, see Finding the MAC Address. If none of your devices have this MAC address, that device might be an intruder.

● In the empty Name field, enter a name for the device. For example, "Amy's PC".

● In the empty MAC Address field, enter the MAC address of the device you're adding to the list.

● Click the ⊕ beside the row.

7. For each device you want to block, repeat step 4.

Tip: You can also block the device from the device list. See Displaying and Blocking Currently Connected Devices (Block List).

Removing a Device From the Allowed or Disallowed Lists

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > MAC Filter**.

5. In the list of allowed/disallowed devices, click the ⊗ beside the row.

6. Click **Submit**.

Wi-Fi Channel

The Wi-Fi channel is the active channel of the Wi-Fi access point. If your network is having performance issues (possibly caused by other Wi-Fi networks in the vicinity using the same channel), try a different Wi-Fi channel.

You can change the channel from your gateway's **Wi-Fi Options** page.

Note: All connected devices will be disconnected and have to reconnect if the channel is changed.

To change the Wi-Fi channel:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > Options**.

5. Select a different channel number in the **Wi-Fi Channel** list, or, to have your device automatically determine the channel to use, select **Auto**.

   Note: If you choose Auto, your device could reselect the same channel. If this happens, try again.

6. Click **Submit**.

Set the Maximum Number of Wi-Fi Devices

You can enter the maximum number of Wi-Fi devices that are allowed to connect to the gateway at the same time.

If your network is having performance issues, you might want to allow fewer Wi-Fi devices to connect to your gateway at the same time, or change the maximum number of devices that can connect to either the Main Wi-Fi or Guest Wi-Fi networks at the same time. (When Guest Wi-Fi is turned on, the maximum number of Wi-Fi devices is shared between Main Wi-Fi and Guest Wi-Fi.)

Note: Your gateway is factory preset to allow a maximum of 64 Wi-Fi devices

Note: If you change the Max Wi-Fi Devices value, the Main Wi-Fi and Guest Wi-Fi values automatically adjust to match the new total.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Wi-Fi > Options**.

5. Beside Max Wi-Fi, select the total number of Wi-Fi devices that can connect to your device at the same time.

   Note: The Main Wi-Fi limit cannot be set to 0.

6. Click **Submit**.

Wireless Distribution System (WDS)

The gateway can act as a wireless base station or a wireless repeater in a wireless distribution system (WDS).

A WDS expands a wireless network through multiple access points. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station. The following figure shows a wireless repeating scenario.

To use the wireless repeating function, your gateway cannot have security enabled and cannot use the auto channel feature.

You must set up a wireless base station and a wireless repeater:

- **Wireless base station**. The router acts as the parent access point that bridges traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater access point. Often, the MAC address is on the product label.

- **Wireless repeater**. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you must know the MAC address of the remote parent access point.

The gateway is always in dual-band concurrent mode, unless you turn off one radio. If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless router or wireless base station, dual-band concurrent mode is not affected.

Before you can set up a wireless network with WDS, both access points must meet the following conditions:

- Use the same SSID, wireless channel, and encryption mode.

- Be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.

- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Set Up the WDS Base Station

You can use the Wireless Repeating Function to set up the base station for a wireless distribution system (WDS).

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You must know the wireless settings for both units. You must know the MAC address of the remote unit. First, set up the base station, then set up the repeater.

To set up the base station:

Both units must be set up using the same wireless settings. The wireless network name (SSID) and the wireless mode must be the same and the wireless security option must be set to None.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Wireless Repeating Function**.

5. Select the **Enable Wireless Repeating Function** check box.

6. Select the **Wireless Base Station** radio button.

7. To prevent wireless clients from associating with the base station and allow LAN client associations only, select the **Disable Wireless Client Association** check box.

   Note: You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.

8. In the Repeater MAC Address 1 through 4 fields, enter the MAC addresses for the access points that should function as repeaters.

9. If your gateway is the base station, it can function as the "parent" for up to four other access points.

10. Click **Submit**.

Your changes are saved.

Set Up a WDS Repeater

You can use the Wireless Repeating Function to set up a repeater for a wireless distribution system (WDS).

Note: Set up the WDS base station first. See Set Up the Base Station.

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

If you are using the router as the base station with a different brand of router or gateway as the repeater, you might need to change more configuration settings. In particular, disable the DHCP server function on the access point that is the repeater.

To configure the gateway as a repeater:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Wireless Repeating Function**.

5. Select the **Enable Wireless Repeating Function** check box.

6. In the Repeater IP Address field, type the IP address of the repeater router.

   Note: This IP address must be in the same subnet as the base station, but different from the LAN IP address of the base station.

7. To prevent wireless clients from associating with the repeater and allowing LAN client associations only, select the **Disable Wireless Client Association** check box.

   Note: You can leave the check box cleared if you prefer wireless clients to be able to associate with the repeater.

8. In the Base Station MAC Address field, enter the MAC addresses for the access point that will be the base station.

9. Click **Submit**.

10. Verify connectivity across the LANs.

A computer on any wireless or wired LAN segment of the gateway can connect to the Internet or share files and printers with any other computer or server connected to the other access point.

GPS Page

From the GPS page, you can obtain your current location coordinates (latitude, longitude, altitude, etc.).

You can also enable or disable GPS tracking, and choose the tracking method being used (one-time or continuous).

Your gateway provides GPS functionality to help you figure out where you are and get you where you're going.

There are a couple of requirements to access the GPS service.

- You must accept the GPS privacy agreement.

- GPS must be enabled.

The GPS service may not be available if you are indoors. (You may be able to get a GPS lock if your device is very close to a window.) GPS receivers must be able to lock onto the global positioning satellites to accurately determine position. The number of obstructions present indoors often makes accurate position determination impossible.

To view or change the GPS settings:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **GPS**.

You can:

- Start or Stop tracking (if GPS Mode is Continuous)

● Update the current location information (if GPS Mode is One-time)

Note: The first time that you access GPS, you will be prompted to read and accept the Location-Based Services (LBS) end user license agreement. You must accept the agreement before you can use the GPS feature.

Note: For best results, minimize the number of obstructions between your device and the GPS satellites.

The following information is displayed.

Item	Description
Most recent position fix	
Update location / Cancel or **Start / Stop**	If the GPS Mode is: ● **One-time**: Click **Update location** to get a location fix, or click **Cancel** to stop waiting for the fix to complete. ● **Continuous**: Click **Start** to begin tracking and refreshing the location fix information regularly, or click **Stop** to stop tracking.
Status	Message indicating what the GPS system is doing (For example, "Tracking a fix", "Searching for satellites", "Inactive")
Time of fix	This is the date and time that the last fix was taken.
Latitude	Latitude at time of last fix. (For example, "N32.51.73")
Longitude	Longitude at time of last fix. (For example, "W105.11.7")
Altitude	Elevation at time of last fix. (For example, "40 meters")
Speed	Speed at which device was moving at time of last fix. (For example, "3.1 mph")
Heading	Direction in which device was moving at time of last fix. (For example, "East")
Satellites	The number of satellites used to get the last fix.
GPS Settings	
Enable GPS	Turns the GPS service on or off. See Enabling / Disabling GPS. **Note:** For best results, minimize the number of obstructions between your device and the GPS satellites.
Use Metric units	This setting specifies whether to use metric units when displaying the GPS results (for example, for altitude, speed, and HEPE). See Using Metric Units.
GPS mode	This setting determines how often your device should obtain a fix. See Setting the GPS Mode.

	● **One-time** – A single fix is used. Use this option if you'll be using your device at the same location. ● **Continuous** – Fixes are obtained every few seconds (also known as auto-tracking). This is useful for turn-by-turn (TBT) navigation applications, such as driving directions, and for NMEA-enabled applications.

Enable or Disable GPS

Before you can access GPS services, you must enable GPS on the gateway's GPS page.

To enable or disable GPS:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **GPS**.

5. In the GPS Settings section, select the **Enable GPS** check box (or clear the check box to disable GPS).

6. Click **Submit**.

Set the GPS Mode

The GPS mode determines how often location fixes are done.

Location fixes can be done:

● Once ("one-time", which can prolong the battery life), or

● Periodically ("continuous")

You can set the GPS mode on the gateway's GPS page:

To set the GPS mode:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **GPS**.

5. In the GPS Settings section beside **GPS Mode**, select the desired mode (**One-time** or **Continuous**).

6. Click **Submit**.

Note: The GPS service must be enabled before you can set the GPS mode. (See Enabling / Disabling GPS.)

Use Metric Units for GPS

You can use metric units in the display of location information (for example, speed and altitude).

You can choose the units on the gateway's GPS page.

Note: The GPS service must be enabled before you can choose the units. (See Enabling / Disabling GPS.)

To specify metric units for the GPS:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **GPS**.

5. In the **GPS Settings** section beside **Use Metric units**, select **Yes** (or select **No** to use standard measurements).

6. Click **Submit**.

Dynamic DNS

Learn about Dynamic DNS (DDNS), a service that lets you access your gateway by using a host name or domain.

A Dynamic DNS (DDNS) service provides a central public database where information (such as e-mail addresses, host names, and IP addresses) can be stored and retrieved. The Dynamic DNS server also stores password-protected information and accepts queries based on e-mail addresses.

If you want to use a DDNS service, you must register for it. The Dynamic DNS client service provider will give you a password or key.

Note: The gateway supports only basic DDNS, and the login and password might not be secure. If you have a private WAN IP address, do not use DDNS service as it can lead to problems

To set up DDNS:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Dynamic DNS**.
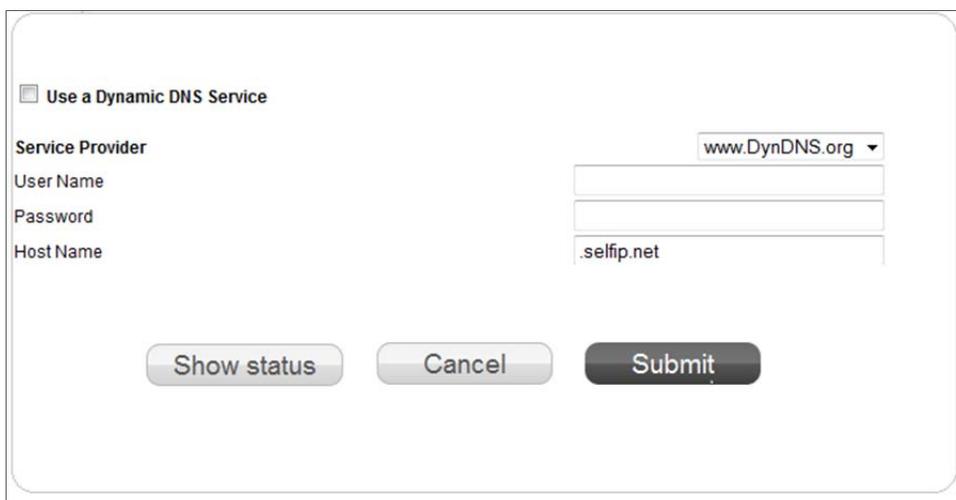
5. If you have registered with a DDNS service provider, select the **Use a Dynamic DNS Service** check box.

6. Select the name of your Dynamic DNS service provider.

7. Type the host name that your Dynamic DNS service provider gave you. (The DDNS service provider might call this the domain name.)

8. Type the user name for your DDNS account.

9. Type the password (or key) for your DDNS account.

10. Click **Submit**.

File Sharing for USB Drives

You can connect a USB drive to the gateway's USB port and share it with others on your network.

You can specify how you want file sharing to be managed for files on a USB device attached to the gateway USB port.

To set up file sharing for a USB drive:

1. Connect a USB drive to the USB port on your gateway.
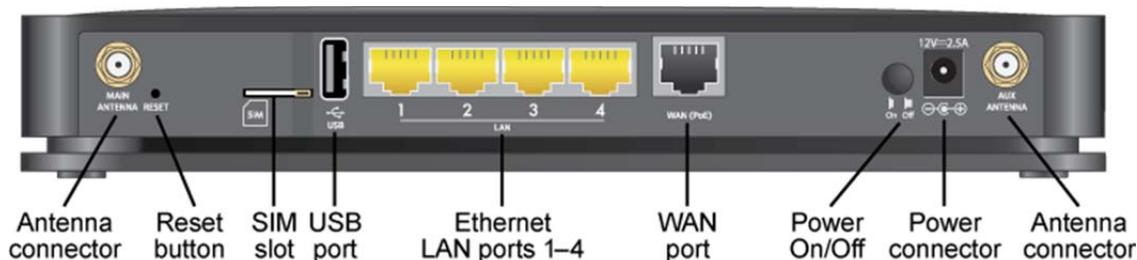
2. On a computer or wireless device that is connected to your gateway, launch a Web browser.

3. In the address or URL field of your browser, type **http://myrouter**.

4. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

5. Click **Settings > File Sharing**.

6. To allow file sharing, select **Enable** in the File Server field.

   When this feature is enabled, all of the files on the USB drive are available as Windows Shared Files to other devices on the local area network (LAN). Shared files are not available to clients on the Internet outside of the local network.

7. In the Domain Name field, specify the network name.

   This feature allows a computer on the LAN to access the share with a name rather than the IP address. The Host Name displays in the Windows Network on local network computers. Files can be accessed with the routers IP address (for example, \\192.168.15.1), the hostname (for example, \\dslrouter), or the link in the network neighborhood.

8. In the File Share Users, specify user names and passwords for access to network file shares.

   With this feature, anyone who tries to access the files on the USB device must enter a user name and password. Each user can be set to read only or have write access to the files on the USB drive. Existing passwords cannot be viewed. You must change it if it is forgotten.

9. To add a user, click the **Add** button and type the user name and password.

10. To edit a user's credentials or password, click the user name.

Gateway Settings

Manage the gateway settings.

Settings

From the Settings page, you can configure your device, network, and router settings.

General

From the General page, you can configure your device's LED status indicators, the gateway's (web browser) URL and administrator password.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General**.

The following information is displayed.

Item	Description
Router LED	
Router LED	Indicates whether the LEDs are used (**On**) or not (**Off**). See Turning the LED On or Off.
Homepage	
(Web UI name) URL	The URL used to show the homepage. See Changing the Gateway's URL.
Set Password	The password used to show the homepage. See Changing the Password.

General > Software and Reset

From this page, you can save your current device settings and restore them later, update your software, reset your device to default settings, and set your device startup options.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

You can:

● Back up and restore your gateway's configuration, if needed. See Export Settings and Import Settings.

● Update your gateway's software. See Update the Software and Firmware.

● Reset some or all of your gateway's settings. See Reset Device Settings Only, Reset the Gateway to Factory Default Settings, and Clear Account Details Only.

The following information is displayed.

Item	Description
Download / Backup	Click **Save** to make a copy (export) of the gateway's current configuration, so that you can restore it later if needed. See Exporting Settings.
Restore Settings	Click **Choose file** to use a previously saved copy of your device configuration. See Importing Settings.
Software Update	Click **Check for update** to see if a new version of software has been released and if there is, download and install it. The last time you checked is shown on the screen (Last checked at). See Update the Software and Firmware. **Note:** Software downloads count against your plan's data limit.
Firmware Update	Click **Upload** to see if a new version of your device's firmware has been released, and if there is, download and install it.
Factory Reset	Click to reset your device to factory default settings and clear your account details. See Reset the Gateway to Factory Default Settings. (You can only do this with assistance from Sprint.)
Reset	**Settings Reset** – Click to reset your device to factory default settings, but leave your Sprint account details unchanged. See Reset Device Settings Only. **Clear Programming** – Click to clear your account details. See Clear Account Details Only.

General > System Logs

Technical support staff may need you to configure system logging in this page for the purpose of error diagnosis.

Note: You should only adjust settings on this page under the direction of technical support staff.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > System Logs**.

System Logs

System logs provide a history of events to troubleshoot errors.

System Logs

Stop Capturing Logs

Save as a File

Clear Log

Logs

syslog: WebServer: Page [/NML_Logs.asp] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:48
syslog: WebServer: Page [/NMLString.asp] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:47
syslog: WebServer: Page [/sprint/nml_data/options_list.xml?_=1380820307247] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:47
syslog: WebServer: Page [/sprint/nml_mapping/menu.xml?_=1380820307134] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:47
syslog: WebServer: Page [/NMLString.asp] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:45
syslog: WebServer: Page [/sprint/nml_data/options_list.xml?_=1380820304952] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:45
syslog: WebServer: Page [/sprint/nml_mapping/omadm_mobile_alerts.xml?_=1380820304919] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:45
syslog: WebServer: Page [/NML_Logs.asp] Access by user admin from IP 192.168.0.18, Thursday,October 03,2013 17:10:42
syslog: WebServer: Page [/NMLString.asp] Access by user admin from IP 192.168.0.18

Mobile Proxy

Mobile Proxy
○ On
○ Off

You can:

● Stop Capturing Logs

● Save as a File

● Clear logs

General > Date & Time Settings

Configure the date and time settings.

To specify the date and time settings:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Date & Time**.

   Note: The Local Time field displays the local time.

5. In the Time Zone field, select the time zone.

6. If your location uses daylight saving, select the **Daylight Saving Time** check box.

   ■ Selecting this check box enables daylight saving time. If the current time falls within the daylight saving period, then daylight saving time takes effect. The Start and End fields display.

7. If needed, change the settings in the Start and End fields.

8. Select or clear the **Automatic Time Update** check box.

■ This check box enables or disables the NTP server. You can edit the first NTP server entry and you can add, remove, or edit a second NTP server.

9. Click **Submit**.

Your changes are saved.

General > MAC Address Cloning

Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address. The format for the MAC address is XX:XX:XX:XX:XX:XX.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > MAC Address Cloning**.

5. If your ISP does not require MAC authentication, select **Use Default MAC Address**.

6. If your ISP requires MAC authentication, select one of the following:

   ▪ **Use Computer MAC address**. Disguise the router's MAC address with the MAC address of the computer that you are currently using to configure the gateway.

   ▪ **Use This MAC Address and manually type the MAC address**. Disguise the router's MAC address with the MAC address of another computer (not the one that you are currently using).

7. Click **Submit**.

General > Remote Management

The remote management feature lets you access your gateway over the Internet to view or change its settings.

You need to know the gateway's WAN IP address to use this feature.

Tip: Be sure to change the password for admin to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See Change the admin Password.

To set up remote management:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Remote Management**.
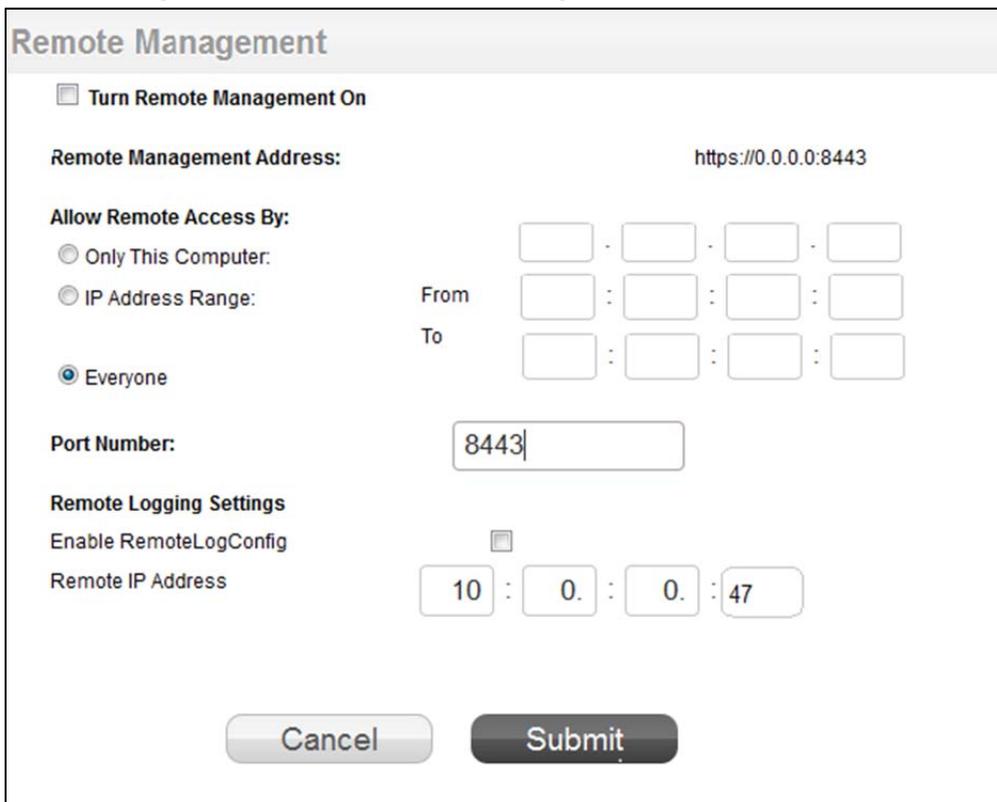
5. Select the **Turn Remote Management On** check box.

6. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the gateway's remote management:

7. For enhanced security, restrict access to as few external IP addresses as practical

8. Select one of the following:

   ▪ To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address to be allowed access.

   ▪ To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. Enter a beginning and ending IP address to define the allowed range.

   ▪ To allow access from any IP address on the Internet, select the **Everyone** radio button.

9. Specify the port number for accessing the web browser interface.

   ■ Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

10. Click **Submit**.

To use remote access:

1. Launch a Web browser on a computer that is not on your home network.

2. Type your gateway's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

For example, if your external address is 134.177.0.123 and you use port number 8080, enter http://134.177.0.123:8080 in your browser.

Network > Setup

From the Network Setup page, you can specify how the gateway selects mobile networks and roaming, and receive network configuration updates from Sprint.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network**.
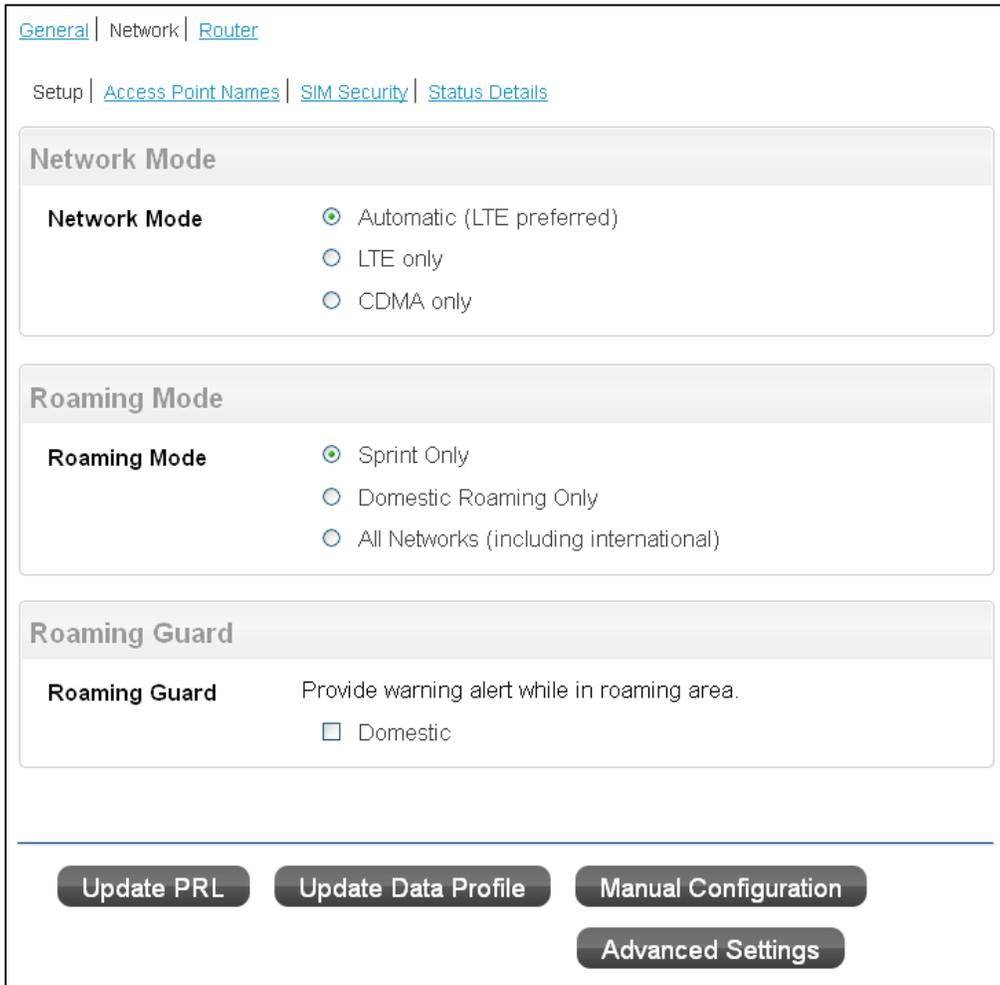
You can:

- Configure network selection and roaming options.

- Check the network for a new Preferred Roaming List.

The following information is displayed.

Item	Description
Network Mode	The type of network that your device can connect to. See Setting the Allowed Network Mode.
Roaming Mode	The areas in which your device can roam. See Setting the Roaming Mode.

Roaming Guard	If selected, the roaming areas where a warning will appear when you enter them. See Enabling / Disabling the Roaming Guard Warning Message.
Update PRL	Click to check if a new PRL (Preferred Roaming List) is available on the network, and use it to update your device.
Update Network Settings	Click to re-run HFA (Hands Free Activation).
Manual Configuration	Use only when instructed by Sprint.
Advanced Settings	Use only when instructed by Sprint.

Network > Access Point Name

In this page, you can add, modify, or remove access point names (APN)s for the networks you want to connect to.

To connect to a carrier's network when roaming, your device must be configured with an Access Point Name (APN) for that carrier. The APN is checked by the carrier to determine the type of network connection to establish.

Note: Your gateway comes with the APN for Sprint preconfigured.

To view or change the access point names:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > APN**.

To add (or modify) an APN, see Configuring Access Point Names.

The list of all APNs that have been set up includes the following information.

Item	Description
Active	The access point currently in use. Only one access point can be marked as active.
Name	Network carrier name (for example, "Sprint").
APN	The operator's access point name (obtained from the operator).
Username	If required, the username (obtained from the operator) used to connect to the APN.
Password	If required, the password (obtained from the operator) used to connect to the APN.
Authentication	The network authentication code (None, PAP, CHAP, PAP or CHAP).

Network > SIM Security

If you are using a SIM that has security enabled, you can disable SIM Security from this page.

This page shows the current status of this security feature, and allows you to disable SIM security if it has been enabled.

Note: The SIM PIN is required to disable SIM Security.

To disable SIM security:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > SIM Security**.
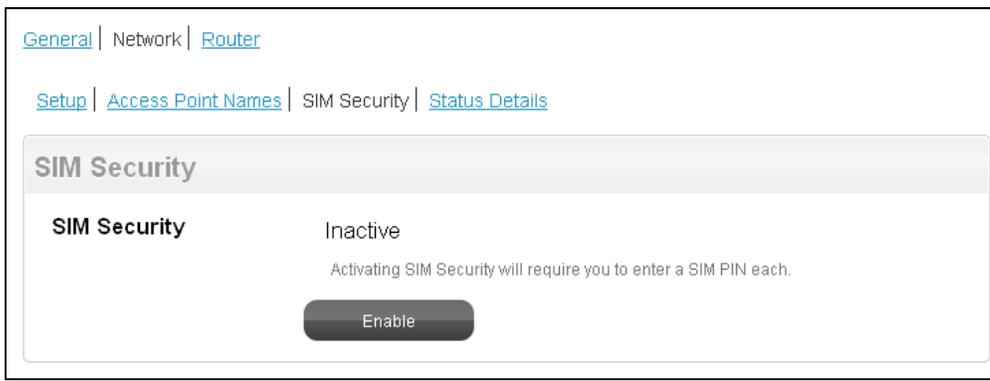
5. If the SIM has security enabled, SIM Security will be Active. Click **Disable** to disable SIM security.

The following information is displayed.

Item	Description
SIM Security	The current state of the SIM PIN feature (Inactive or Active). Click **Disable** to disable SIM security.

Network > Status Details

This page shows you details about the current mobile broadband connection (3G or LTE).

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > Status Details**.

The information that is displayed depends on your current connection.

4G/LTE Details

Item	Description
Connected Status	Indicates whether you are connected to an LTE network.
Service type	Indicates the LTE service type.
RSRP	The signal strength of the LTE network. (Reference Signal Received Power)
RSRQ	The siqnal quality of the LTE network (Reference Signal Received Quality). RSRQ is the ratio between the RSRP and the Received Signal Strength Indicator (RSSI).
RS-SINR	Signal to Interference Noise Ratio based on Reference Signals (narrowband and wideband)
PLMN ID	

Serving Cell	
TX Power	The transmitter power. A higher number is better.
IP Address	The IP address of the 4G LTE connection.
Channel UL	The channel that is used to upload to the 4G LTE network.
Channel DL	The channel that is used to download from the 4G LTE network.
IMSI	The International Mobile Station Identity is an identifier of a device on the network.
Band	The LTE band being used for the connection.
Last Error Code	Technical support staff may request this value from you.
ICCID	The Integrated Circuit Card ID.

3G Details

Item	Description
Status	Indicates whether you are connected to a 3G network.
PS service type	Indicates the 3G service type (for example, CDMA, HRPD, CDMA_HRPD).
IP Address	The IP address of the 3G connection.
Coverage Type	The type of 3G network available.
RSSI	Signal strength of the network.
Ec/Io	Dimensionless ratio of the average power of a channel, typically the pilot channel, to the total signal power.
MDN	Mobile Directory Number. This is your 10-digit telephone number.
MSID	Mobile Station Identifier.
DRC Cover	Digital Rate Control Cover.
DRC Value	Digital Rate Control Value.

Channel	DRC Channel number.
Roaming	Indicates if you are roaming on Sprint, domestically, or internationally.
PRL Version	Preferred Roaming List version. To update the PRL, see Network Page.
1xRTT PN	Technical support staff may request this value from you.
EVDO PN	Technical support staff may request this value from you.
PRev	Technical support staff may request this value from you.
Rx Power	Technical support staff may request this value from you.
Serving SID	The Serving System ID identifies your home network area and is used to determine if you are 'home' or 'roaming'.
NID	Technical support staff may request this value from you.
Packet Zone ID	Technical support staff may request this value from you.
Frame Error Rate	Used to determine the quality of a signal connection. Technical support staff may request this value from you.
Subnet Color Code	Technical support staff may request this value from you.
AN-AAA	Technical support staff may request this value from you.
Packet Error Rate	Technical support staff may request this value from you.
MIP Error Code	The Mobile IP Error Code. Technical support staff may request this value from you.

Network > Broadband Settings (Dual WAN)

This page is used to configure the broadband dual WAN Settings.

The default setting is to always use mobile broadband.

To specify broadband settings:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > Broadband Settings**.

Available options are:

- Used Fixedline Connection first if fails use Mobile Broadband Connection.

- Always use Fixedline Broadband Connection.

- Always use Mobile Broadband Connection

Router > Basic

From this page you can configure the router's UPnP feature, LAN settings, and DMZ settings.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.
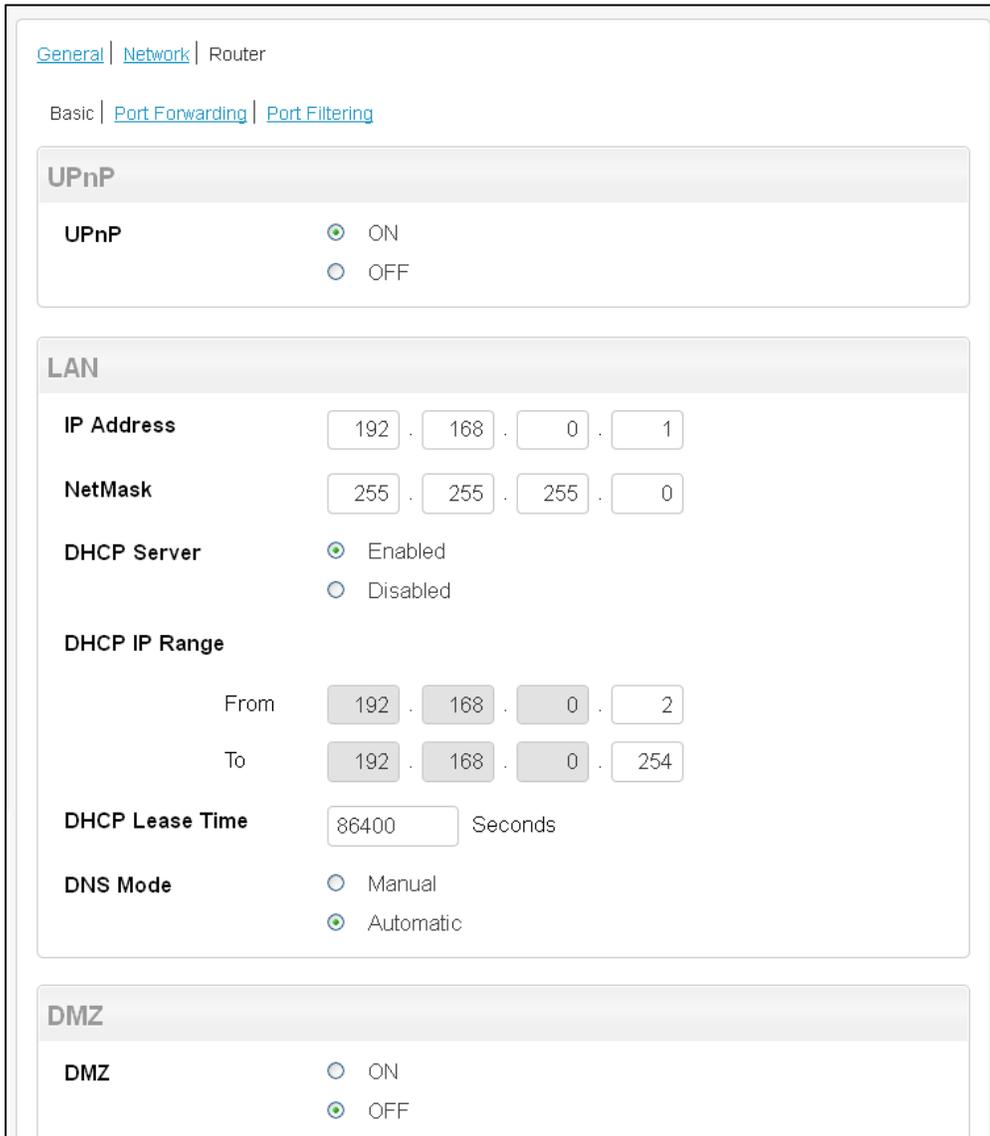
5. You can make changes to any of these fields. When you finish, click **Submit**.

The following information is displayed.

Item	Description
UPnP	
UPnP	Current state of the Universal Plug and Play feature (On or Off). (See UPnP (Universal Plug and Play).)

LAN	
IP Address	The routing hardware's IP address on the LAN.
Netmask	The routing hardware's internal LAN subnet mask.
DHCP Server	This field enables (On) or disables (Off) DHCP. See DHCP.
DHCP IP Range	This specifies the starting and ending address of the range of IP addresses available for your device to dynamically (that is, not permanently) assign to computers connected to it. See DHCP.
DHCP Lease Time	This is the amount of time, in minutes, a computer can use its assigned IP address before it is required to renew the lease. After this time is up, the computer is automatically assigned a new dynamic IP address. See DHCP. Enter a number between 2 and 10080.
DNS Mode	This specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained. **Manual:** The routing hardware assigns DHCP clients the DNS servers specified in the **DNS 1** and **DNS 2** fields Use this option to access a DNS server that provides customized addressing or if you have a local DNS server on your network. **Note:** The **DNS 1** and **DNS 2** fields appear only if **DNS Mode** is Manual. **Auto**: The DNS server specified by Sprint is used.
DMZ	
DMZ On/Off	Enable / disable demilitarized zone.
DMZ Address	If DMZ is enabled, this is the IP address of a single computer used to receive all unsolicited incoming connections.
Submit	

Router > Port Forwarding

Port forwarding lets you forward incoming traffic to specific ports and devices (per their local IP address) on your network. (Normally, incoming traffic is blocked.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Forwarding**.

You can:

- Enable or disable port forwarding. See Enable Port Forwarding.

Note: You must enable port forwarding before you can view and update the port forwarding list.

- Enter port forwarding details for an application. (See Enable Port Forwarding for an Application.)
  For example, you can configure port forwarding so that:

  - You can access your Remote Desktop from the Internet (by specifying the WAN [public] IP address that your device is using).

  - Internet users can access a Web, FTP, or email server, or gaming or Internet application hosted by your computer.

- Remove an application from the port forwarding list. (See Port Forward Panel: Disable Port Forwarding for an Application.)

Note: Port forwarding creates a security risk. When not required, port forwarding should be disabled.

Note: Port forwarding does not apply to normal browsing, file downloading, running most online games or other applications hosted on the Internet. (Some online games require port forwarding.)

The following information is displayed.

Item	Description
Port Forwarding	Indicates whether port forwarding is on (Enable) or off (Disable).
List of forwarded ports: This list appears only if port forwarding is on. Each port displays:	
Name	A name describing the application using the port.
IP Address	The IP address of the server being accessed.
Port	The port that is forwarded. If the application uses more than one port, each port must be forwarded separately.
Protocol	The protocol (TCP, UDP, etc.) being used for this application.
Actions	

Router > Port Filtering

Port filtering lets you either allow (white list) or prevent (black list) which applications (for example, http, ftp, email servers) can access the Internet.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Filtering**.

You can:

- Enable port filtering. (See Port Filtering Panel: Enable Port Filtering.)

- Add an application to a port filtering list. (See Port Filtering Panel: Enable Port Filtering for an Application.)

- Remove an application from the port filtering list. (See Port Filtering Panel: Disable Port Filtering for an Application.)

The following information is displayed.

Item	Description
Port Filtering	Indicates which type of filtering is being used. - **No Filtering**: All applications are allowed to access the Internet. - **Black List**: Applications in the list are not allowed to access the Internet.
List of filtered ports: This list appears only if port filtering is on. Each port displays:	
Name	A name describing the application using the port.
Port	The port that the application uses to access the Internet.
Protocol	The protocol (TCP, UDP, etc.) being used by the application.
Actions	

Router > Address Reservation

Address reservation lets you specify a specific IP address that the gateway assigns to a computer or device when it connects to the gateway's local area network (LAN).

When you specify a reserved IP address for a computer on the gateway's local area network (LAN), that computer always receives the same IP address each time it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Address Reservation**.

5. Click the ⊕ Add button.

6. Select the radio button of the computer in the Reservation Table.

7. If the computer is not on the Address Reservation Table, enter the IP address, MAC address, and device name of the computer you want to add.

8. Click the ⊕ **Add** button when finished.

To edit a reserved IP address:

1. Select the radio button next to the reserved address.

2. Click the **Edit** button.

3. Edit the IP address, MAC address, or device name.

4. Click the **Accept** button when finished.

To delete a reserved IP address:

1. Select the radio button next to the reserved address.

2. Click the ⊗ **Delete** button.

Error! Bookmark not defined. Router > ALG

This page is used to configure the ALG Services.

Note: When the firewall level is set to High, some services may not be configurable.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > ALG**.
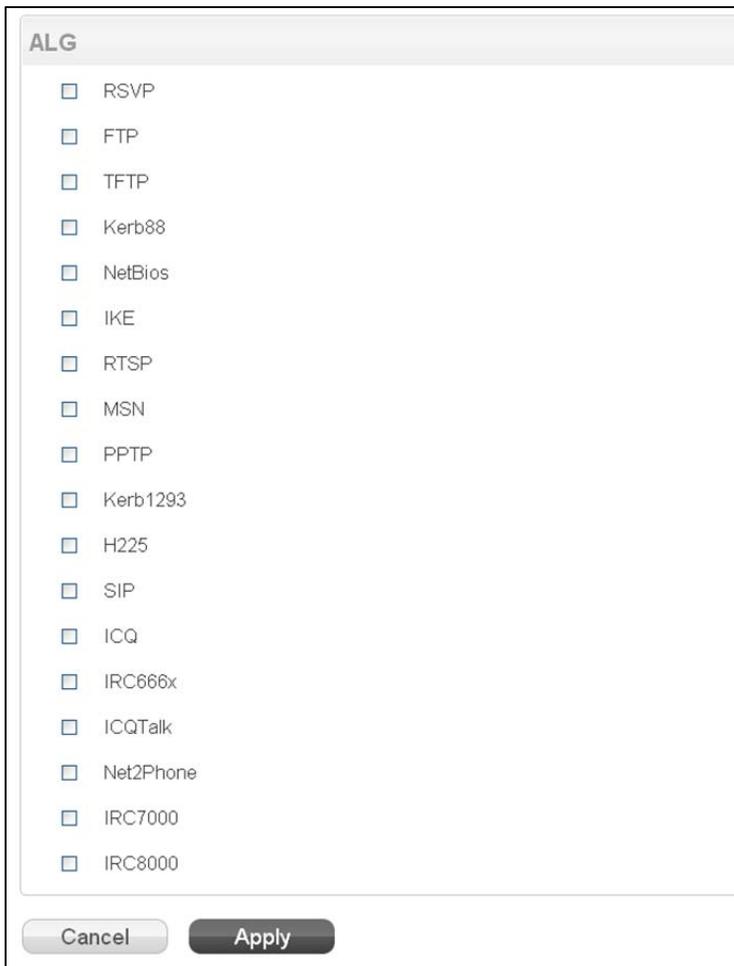
5. Select the check boxes for the ALG services that you want.

6. Click the **Apply** button.

Firewall Rules

The Firewall Rules page sets the level of security on your local network.

You can:

- Specify the security level for your network

- Enable or disable Port Scan

- Enable or Disable DoS protection

To specify the firewall security level:

All security levels, except "None," protect against known Internet attacks and attempts at remote access to your modem.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Firewall Rules**.

6. Select the radio button for the security level that you want.

7. Click the **Apply** button.

The following settings are available.

Item	Description
High	The high security setting only allows basic Internet functionality. The High security setting guarantees to only pass Mail, News, Web, FTP, IPSEC and Telnet. All other traffic is not allowed. High security restricts modification by NAT configuration options.
Medium	The medium security setting only allows basic Internet functionality by

	default, just like High level security. Medium security, however, allows customization through NAT configuration so certain traffic can pass
Low	The low security setting will allow all traffic except for known attacks. With low, your modem is visible by other computers on the Internet
Custom	Custom is an advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this

To enable or disable Port Scan:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Firewall Rules**.

5. Select or clear the **Enable Port Scan** check box.

6. Click the **Apply** button.

To enable or disable Denial of Service (DoS) protection

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Firewall Rules**.

5. Select or clear the **Enable DoS Protection** check box.

6. Click the **Apply** button.

Support

This page provides links to resources that can help you use your device and manage your Sprint account.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click the **Support** link in the top right corner.
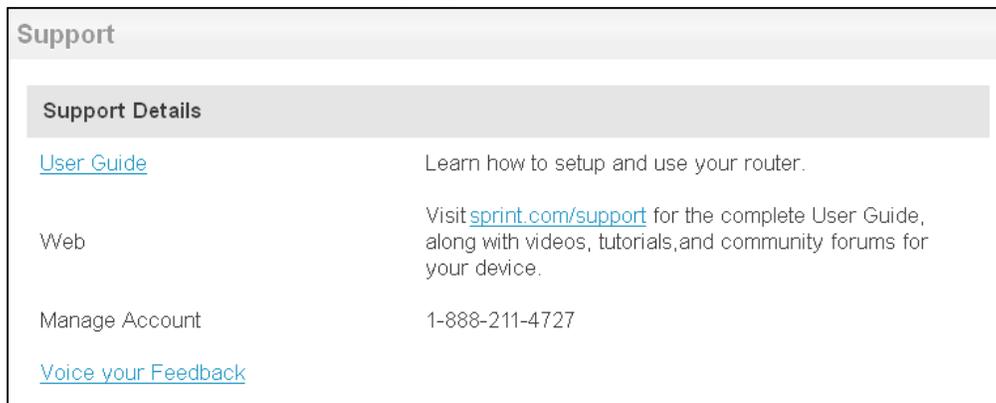
The following information is displayed.

Item	Description
User Guide	Open an online copy of this guide in a new Web browser window or tab. (You must be connected to the Internet to use this link.)
Web	Click the link to open the online support website in a new Web browser window or tab where you can find a variety of resources to help you with your gateway. (You must be connected to the Internet to use this link.)
Manage Account	Contact Sprint Customer Service by telephone (for business use or personal use).
Voice Your Feedback	Send NETGEAR your comments on your device. See Feedback Page.

About

View information about your device and account.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click the **About** link in the top right corner.

Account Details		Device	
My Number:	9132275139	Model:	LG6100D-1SNNAS
IMEI:	357595050001534	Router URL:	http://myrouter
ESN:	804E0FED	Firmware:	VER:02.02.26
ICCID:	89011200000188124183	Firmware Date:	Sep 24 2013 15:37:01
		Bootloader Version:	VER:02.01.24

Wi-Fi Details (2.4GHz)		Wi-Fi Details (5GHz)	
Wi-Fi Name:	LG6100D-F096	Wi-Fi Name:	LG6100D-5G-F096
Wi-Fi MAC:	04:A1:51:85:F0:96	Wi-Fi MAC:	06:A1:51:85:F0:96
Wi-Fi IP Address:	192.168.0.1	Wi-Fi IP Address:	192.168.0.1
Wi-Fi Security Type:	None	Wi-Fi Security Type:	None
Wi-Fi Range:	Short	Wi-Fi Range:	Short
SSID Broadcast:	Yes	SSID Broadcast:	Yes

Firmware		Network	
Firmware Version:	NTG9X15C_45.02.08.00	View Network Status Details	
Build Date:	2013/09/05 11:39:10		
PRI Version:	00.07		

You can:

● Save the image on this page to a file on your computer. Click **Save as a file**.

The following information is displayed.

Item	Description
Account Details	
My number	The gateway's telephone number.
IMEI	International Mobile Equipment Identify number.
ICCID	The serial number of the SIM.

Wi-Fi Details	
Wi-Fi Name	The Main Wi-Fi network name. (See also Change Wi-Fi Network Names and Passwords.)
Wi-Fi MAC Address	The MAC address of the LTE module. Each wireless device has a unique MAC address (assigned by its manufacturer).
Wi-Fi Security Type	The security standard used for the Wi-Fi network. (See Wi-Fi Security.)
Wi-Fi Range	
SSID Broadcast	Indicates whether the SSI D (Wi-Fi network name) is being broadcast. (See Options Section.) You could choose to not broadcast, and give the Wi-Fi name directly to users.
Firmware	
Firmware Version	The gateway's firmware version.
Build Date	The date the firmware version was created.
PRI Version	The PRI version.
Network Status	
View Details	Click the link to jump to the Network > Status Details Page.

Feedback

Use the links on this page to send your comments on your device, look up support information, and participate in a customer survey.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click the **Feedback** link in the bottom left corner of any page.

The following information is displayed.

Item	Description
Connect with us	
Facebook	Click to view the AirCard Facebook page in a new browser window or tab. (Your device must be connected to the network for this option to work.)
Twitter	Click to view the AirCard Twitter feed in a new browser window or tab. (Your device must be connected to the network for this option to work.)
Product Support	
User Guide	Open an online version of this user guide in a new window or tab.
FAQs	Read frequently asked questions and answers.
Survey	
Customer Feedback Survey	Participate in a NETGEAR customer survey.

Ethernet WAN Settings

Your gateway has an Ethernet WAN port on the rear panel. You can use an Ethernet cable to connect the gateway to Internet service.

Connect the Ethernet WAN Port

You can connect the gateway to a cable or DSL modem with an Ethernet cable and set up the router to use that modem's Internet service instead of the mobile service.

To install the gateway with an Ethernet Internet connection:

1. Prepare your modem.

   - Unplug your modem's power.

   - If the modem has a battery backup, remove its batteries.

   - If your modem was already connected to another router, disconnect the cable between your modem and that router.

   - Make sure that your modem is turned off and is cabled only to the wall jack for your Internet service.

2. Connect your modem.

3. Plug in, then turn on your modem. (Replace the batteries if you removed them.)

4. Use an Ethernet cable to connect your modem to the Ethernet WAN port of your gateway.

| Antenna connector | Reset button | SIM slot | USB port | Ethernet LAN ports 1–4 | WAN port | Power On/Off | Power connector | Antenna connector |
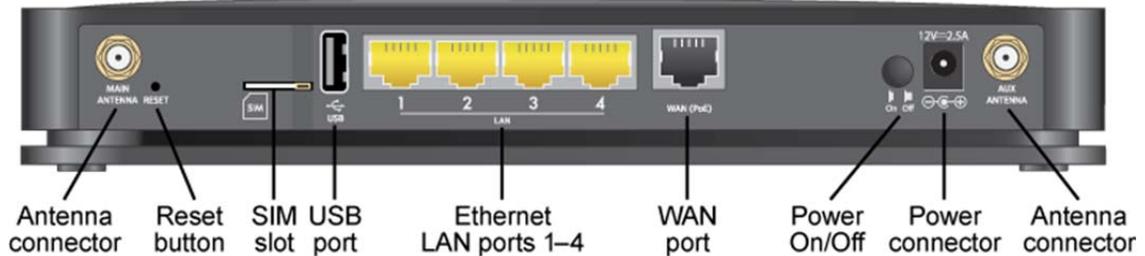
5. Connect the power adapter to the gateway, and plug the power adapter into an outlet.

6. If no LEDs are lit, press the **Power On/Off** button on the rear panel of the gateway.

   ▪ The **Power** ⏻ LED lights.

   ▪ When the gateway connects to the Internet, the **Ethernet WAN** �֎ LED lights.

Specify WAN Settings

The WAN Setup screen lets you configure advanced settings for the Ethernet WAN port.

To specify WAN settings:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > WAN Setup**.

5. Specify the following settings:

- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This feature should be disabled only in special circumstances.

- **Respond to Ping on Internet Port**. If you want the gateway to respond to a ping from the Internet, select this check box. Use this feature only as a diagnostic tool because it allows your gateway to be discovered. Do not select this check box unless you have a specific reason.

- **Disable IGMP Proxy**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.

- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. Reduce the MTU only if you are sure that it is necessary for your ISP connection.

6. Click **Submit**.

MTU Size

Learn about maximum transmission unit (MTU) size and how to change this setting.

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path has a lower MTU setting than the other devices, the data packets must be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for your gateway is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP recommends changing the MTU setting. These web-based applications might require an MTU change:

- A secure website that does not open, or only part of a web page displays

- Yahoo! Mail

- MSN portal

- America Online's DSL service

- You use VPN and have severe performance problems.

- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

- An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

The following table lists common MTU sizes.

MTU Size	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR gateways, adapters, and switches
1492	Used in PPPoE environments
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	1400 Maximum size for AOL DSL.

576	576	Typical value to connect to dial-up ISPs.

Change the MTU Size

The default MTU size usually works, but you can change the MTU size.

To change the MTU size:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > WAN Setup**.

5. In the MTU Size field, enter a value from 64 to 1500.

6. Click **Submit**.

LED Settings

By default, the LEDs are on because they are status indicators. You can log in to the gateway and turn the LEDs off and on.

To turn the LEDs off and on:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Device**.

5. Beside **LED**, select **On** or **Off** as desired.)

6. Click **Submit**.

Router Settings

Adjust your gateway's router settings through the Basic, Port Forwarding, and Port Filtering pages.

UPnP (Universal Plug and Play)

UPnP provides simple and robust connectivity among consumer electronics, intelligent appliances, and mobile devices from many different vendors. (For more information, see upnp.org.)

Note: If UPnP is enabled, there are potential security risks.

To enable UPnP:

Before you can use UPnP, you must enable it.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.

5. Next to **UPnP**, select **On**.

6. Click **Submit**.

DHCP

DHCP (Dynamic Host Control Protocol) automatically assigns an IP address to each device on the network and manages other network configuration information for devices connected to your network. You do not need to manually configure the IP address on each device that's on your network.

The assigned IP addresses are not permanent (as opposed to when using static IP).

Most ISPs (Internet Service Providers) use DHCP.

Normally, you should enable DHCP, in which case you must configure each device on the network with one of the following:

- TCP/IP settings set to "Obtain an IP address automatically."

- TCP/IP bound to the Ethernet connection with DHCP.

If DHCP is disabled, you must configure each device on the network with:

- Fixed (permanent/static) IP address.

- DNS server addresses (provided by Sprint).

To enable DHCP:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.

5. Next to **DHCP Server**, select **Enabled**.

6. You can set the following DHCP settings:

●   DHCP IP Range: This is the starting and ending address of the range of IP addresses available for your device to dynamically (that is, not permanently) assign to computers connected to it.

   The start address must be 192.168.0.10 or above and the ending address must be 192.168.0.50 or below.

●   **DHCP Lease Time**: This is the amount of time, in minutes, a computer can use its assigned IP address before it is required to renew the lease. After this time is up, the computer is automatically assigned a new dynamic IP address.

   Note: Enter a number between 2 and 10080.

●   **DNS Mode** — This specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained. (See DNS Mode.)

7. Click **Submit**.

DNS Mode

The DNS Mode setting specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.

5. Set **DNS Mode** to one of the following:

- **Auto**: The DNS server specified by Sprint is used.

- **Manual**: The routing hardware assigns DHCP clients the DNS servers specified in the **DNS 1** and **DNS 2** fields. (These fields appear when **Manual** is selected.) Use this option to access a DNS server that provides customized addressing or if you have a local DNS server on your network.

6. Click **Submit**.

Enable Port Forwarding

Before you can use or configure Port Forwarding, you must enable it.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Forwarding**.

5. Next to **Port Forwarding**, select **Enable**.

6. Click **Submit**.

Enable Port Forwarding for an Application

You can enable port forwarding for certain application types.

Note: Port forwarding must currently be enabled. (See Enabling Port Forwarding.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Forwarding**.

5. In the blank row of the list, enter a Name that describes the application (for example, "RandomEmailApp").

6. In the **IP** field, enter the IP address of the server to be accessed.

7. In the **Port** field, enter the port used by the application. (If the application uses more than one port, each port must be forwarded separately.)

8. In the **Protocol** list, click the protocol(s) used for this application (TCP, UDP).

9. Click the ⊕ to add this row to the list.

10. Click **Submit**.

Disable Port Forwarding for an Application

If you want to stop forwarding any ports, you can remove them from the forwarding list.

Note: Port forwarding must currently be enabled. (See Enabling Port Forwarding for an Application.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Forwarding**.

5. Click the ⊗ beside the row that you want to remove.

6. Click **Submit**.

DMZ – General

You can select one computer to receive all unsolicited incoming connections.

The IP address of the DMZ ("demilitarized zone") is the default recipient of incoming packets (from the Internet) that are not handled by port forwarding rules or NAT'd connections:

● If port forwarding is enabled, incoming traffic is routed according to the port forwarding rules or NAT'd connections.

● If incoming traffic was not routed as a result of the above:

▪ If DMZ is enabled, then incoming traffic is routed to the computer that uses the IP address specified by the DMZ settings.

▪ If DMZ is not enabled, the incoming traffic is blocked.

Note: Putting a computer in the DMZ opens all the ports of that computer, and exposes that computer to various security risks. Use this option only as a last resort — if possible, use other options instead (for example, port forwarding).

Enable DMZ

Before you can use or configure DMZ, you must enable it.

Error! Reference source not found. 84

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.

5. Next to **DMZ Enabled**, select **ON**.

6. Click **Submit**.

Configure DMZ

Specify which computer is to receive all unsolicited incoming connections.

Note: DMZ must currently be enabled. (See Enable DMZ.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Basic**.

5. In the **DMZ Address**, enter the IP address of the computer that you want exposed to the Internet. (If you don't know how to find the IP address, see Finding the IP Address.)

Enable Port Filtering

Before you can use or configure Port Filtering, you must enable it.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Filtering**.

5. In the **Port Filtering** list, select **Black List** to prevent specific applications from using the Internet.

6. Click **Submit**.

Error! Reference source not found.   85

Enable Port Filtering for an Application

You can enable port filtering for certain application types.

Note: Port Filtering must currently be enabled. (See Port Filtering Panel: Enabling Port Filtering.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Filtering**.

5. In the **Name** field, enter a name that describes the application being filtered (for example, "RandomEmailApp").

6. In the **Port** field, enter the port used by the application.

7. In the **Protocol** list, click the protocol(s) used for this application (TCP, UDP, or both).

8. Click the to add this filter to the list.

9. Click **Submit**.

Disable Port Filtering for an Application

If you currently have port filtering enabled and some ports already in the list (Black List or White List), you can remove any of those rows.

Note: Port Filtering must currently be enabled. (See Port Filtering Panel: Enable Port Filtering.)

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Router > Port Filtering**.

5. Select **Black List**.

6. To remove an application from the list click the beside the row that you want to remove.

7. Click **Submit**.

Login Settings

You can customize the URL that you use to log in to the gateway and you can change the administrator password.

Change the Gateway URL

You may want to change the URL for the gateway to something more memorable.

To change the URL:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Device**.

5. In the **URL** field (in the **Homepage** section), type the new value (maximum 31 letters and numbers).

6. Click **Submit**.

Change the admin Password

For security reasons, you should change the gateway's admin password on a regular basis.

It is strongly recommended that you enable password recovery, so that if you forget the password you can recover it.

Note: If you forget the admin password and you have not enabled password recovery, you'll need to reset your device to its default settings and go through the device setup. (See What Do I Do if I Forget the Administrator Password?)

To change the administrator password and enable password recovery:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Device**.

5. In the **Old Password** field, type the old password.

6. In the **New Password** field, type the new password (1–31 letters, numbers, and symbols).

7. In the **Confirm New Password** field, type the new password again.

8. Select the **Enable Password Recovery** check box.

9. Select two security questions and provide answers to them.

10. Click **Submit**.

Mobile Network Settings

View information about your mobile network activation, data usage, and settings.

View Network Activation Information

You can check whether network access is activated.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **About** in the top right corner of the page.

5. Check the **Activation Date** in the WWAN Info section. This is the date that the gateway was activated on the Sprint network.

View Data Usage

You can view an estimate of your data usage on your device's home and Data Usage screens, and on the gateway's home page.

Note: The data usage shown is an estimate only and is not accurate for billing purposes.

Note: The session data counter resets automatically each time your device is powered off and on, and when the mobile broadband network connection disconnects and reconnects (for example, when going through a tunnel). The billing plan data counter resets automatically when the next billing cycle starts.

To view an estimate of your data usage:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

The Data Usage **Session** section displays:

- Amount of data used in the current session.

- The length of time the connection has been active.

The Data Usage **Billing Cycle** section displays:

- Total amount of data used in the current billing cycle, and amounts used for each network type

- Number of days remaining in the current billing cycle.

- Date that the next billing cycle begins.

- **Check Carrier Usage** – Click to connect to Sprint's website and view detailed billing plan information.

Network Settings

Adjust your device's network settings to select the network types that can be connected, and set roaming options.

Set the Roaming Mode

Use this feature to choose where your device can be used in roaming mode.

You can adjust this setting on your gateway's **Settings > Network > Setup** page, using the following options:

- **Sprint Only** – Your device can be used only in Sprint service areas.

- **Domestic CDMA (Including Sprint)** – Your device can roam only in North America.

- **Any Network** – Your device can roam anywhere in the world.

To set the roaming mode:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network**.

5. Beside **Roaming Mode**, select the desired value.

6. Click **Submit**.

Enable or Disable the Roaming Guard Warning Message

Use this feature to have your device display a warning when you enter a roaming area.

To enable or disable the roaming guard warning message:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network**.

5. Beside Roaming Guard, select the warnings you would like to display (Domestic and/or International).

6. Click **Submit**.

Set the Network Mode

Use this feature to select the types of networks that your device can connect to.

You can adjust this setting on the gateway's **Settings > Network** page, to one of the following options:

- **Automatic (LTE preferred)** – The connection will be established on the fastest available network.

- **LTE only** – The connection can be established **only** on an LTE network. Your device **will not** connect to CDMA networks.

- **CDMA only** – The connection can be established **only** on a CDMA (3G) network. Your device **will not** connect to LTE networks.

To set the network mode:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network**.

5. Beside Network Mode, select the desired network mode that your device can connect to.

6. Click **Submit**.

Configure Access Point Names

Your gateway comes preconfigured with the Access Point Name (APN) for Sprint.

To add an APN for another network:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > Access Point Names**.

5. In the blank line, enter the APN details:

● **Active**: If the new APN is going to be used now, select this button.

● **Name**: Enter a short description (for example, the carrier name).

● **APN**: Enter the APN you obtained from the carrier.

● **Username**: Enter the username you obtained from the carrier (if required).

● **Password**: Enter the password you obtained from the carrier (if required).

● Select the **Authentication** mode to be used (**None**, **PAP**, **CHAP**, **PAP or CHAP**).

6. Click **Submit**

7. Click the ⊕ beside the new APN entry.

To select the APN to be used:

■ Select the **Active** button at the beginning of the entry.

To remove an APN from the list:

■ Click the ✖ beside the APN entry.

Software and Reset

Export and Import Settings

You can save your gateway settings so that you can make changes to your configuration and, if necessary, restore the original settings.

Export Settings

Settings include configuration information for your gateway and its Wi-Fi networks.

You can, for example, export (save) the current configuration, then make some changes and test them. You can then import (restore) the saved configuration.

To export the settings to a text file:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. In the **Download / Backup Settings** section, click **Save as**.

6. Save the file to an appropriate location in your computer. By default, the file (export.cfg) is saved to your Downloads folder.

Import Settings

This feature lets you restore a saved configuration.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. In the **Restore Settings** section, click **Browse**.

6. Navigate to the folder where your previously saved configuration file is stored.

7. Click **Open** to restore your device with the imported settings.

Note: Your device may reset, and you may need to reconnect to Wi-Fi and the Internet. (See How Do I Connect to Wi-Fi? and Launching Your Network Connection.)

Update the Software and Firmware

From time to time, updates may become available for your gateway, and your gateway will receive an alert. You can also check for new updates manually.

The updates may improve performance and add or modify features. The updates may include the following:

- Firmware

- Software

- Other files

Download Software Updates

You can download software updates from your device or from the web page.

When a software update becomes available:

- If your device is connected to Sprint's LTE network, the update downloads automatically and an Alert message appears on the home page. Click **Install now** to install the update. Your device reboots automatically to use the new software. Any devices that were previously connected will have to be reconnected.

- If your device is connected to Sprint's 3G network, an Alert message appears on you're the home page. Click **Download now** to download and install the software update. Your device reboots automatically to use the new software. Any devices that were previously connected will have to be reconnected.

You can also check for updates manually without having received an alert.

There are two ways to get the software update. You can get it from the Alert message, or from the Software and Reset page.

To get the update from the Alert:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. In the Alert message for the available update, click **Install Now**.

5. Follow the onscreen instructions.

To get the update from the Software and Reset page:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. Click **Check for update**. If an update is available, an **Install Now** button appears.

6. Click **Install Now**.

7. Click **Continue**.

Upgrade Firmware from a File

A one-click tool may be available for upgrading firmware from a file in enterprise environments. Contact Sprint for details.

Reset Your Gateway

In some cases, you may want or need to clear your account information to use your gateway with another account, reset most settings (except for your account and network activation), or reset your device to its factory default settings.

You can clear these settings from your device's Reset screen, or from the gateway's Software and Reset page.

Clear Account Details Only

If you want to use your device with another account, you need to clear your current account.

You can clear these settings from your gateway's Reset page, or from the Software and Reset page.

Note: All connected devices will be disconnected and your device will reboot automatically. You will have to activate your device with your new account before they can reconnect.

To clear account details:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. Below **Clear Programming**, click **Reset**.

6. Click **Begin Reset**.

Reset Device Settings Only

If you want to reset your device to its default behavior, but don't want to change your account or network activation, you need to reset your device settings.

You can reset these settings from your gateway's Reset page or from the Software and Reset page.

Note: All connected devices will be disconnected and your device will reboot automatically. After the reset finishes, they can reconnect.

To reset device settings:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. Below **Settings Reset**, click **Reset**.

6. Click **Begin Reset**.

Reset the Gateway to Factory Default Settings

In some cases you will need to reset your device's software to its factory default settings.

WARNING: If you reset the software to default settings, you must go through the device setup, as if you've just purchased your device. (See Starting Your Device for the First Time.)

You'll need to reset the software to default settings if:

● You've forgotten the administrator password.

● You've changed the DHCP settings such that your device is inoperable. (For example, there's no communication with your device.)

You can reset your device to factory settings from the gateway's Software and Reset page.

Note: All connected devices will be disconnected and your device will reboot automatically.

To reset the gateway to its factory settings:

Note: You can only do a factory reset of your device with Sprint's assistance. Contact Sprint Customer Service to obtain an SPC code that you will need to enter to perform the reset.

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > Software and Reset**.

5. Below **Factory Reset**, click **Reset**.

6. Enter the SPC code provided by Sprint, then click **Submit**.

7. Click **Begin Reset**.

Set Up a Virtual Private Network (VPN)

Learn about and set up virtual private network (VPN) client-to-gateway and site-to-site tunnels.

A VPN is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users an access to a central organizational network. You need networking knowledge to implement these features.

VPN Overview

Learn about VPN client-to-gateway VPN tunnels and site-to-site VPN tunnels, which use IPSec IKEv1 (PSK/XAuth).

- **Remote-client to gateway VPN**. The gateway must be connected to the public network either through DSL or a WAN uplink. Remote users on the Internet can create an IPSec tunnel from their computers to the gateway using the WAN IP address of the gateway. Once connected, the remote users can access the LAN-side resources of the gateway.

  The gateway supports the following clients:

  - NETGEAR ProSAFE VPN Client VPNG01L/VPNG05L Professional Software Version 5.14.003, available here: http://kb.netgear.com/app/answers/detail/a_id/20316

  - IPSecuritas VPN client Version 3.4 for MAC OS platforms from Lobotomo Software, available here: http://www.lobotomo.com/products/IPSecuritas/

- **Site-to-site VPN**. You can establish an IPSec tunnel between two gateways. The LAN-side users from either gateway can access the other through the site-to-site tunnel. When you are configuring the site-to-site tunnel, each gateway must have a unique IP address range for its LAN side.

Set Up a Remote Client-to-Gateway VPN

To set up a remote client-to-gateway VPN, you must complete the following tasks:

1. Add the VPN users (the remote client users).

2. Specify the VPN connection information.

3. Enable the VPN.

4. Use VPN client software to configure the remote clients.

Add VPN Users

The VPN users are the remote users for client-to-gateway VPN tunnels.

To add VPN users:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > VPN**.

5. In the VPN Users section, click the **+** (Add) button.

6. Enter the user name and password.

7. Click the **Save** button.

   The new VPN user displays on the Manage VPN Connection screen.

To edit a VPN user:

1. Select the VPN user from the VPN Users list.

2. Click the **Edit** button.

3. Type the changes for the user name and password

4. Click the **Save** button.

The changes are saved.

To delete a VPN user:

1. Select the VPN user from the VPN Users list.

2. Click the **Delete** button.

The user is removed from the VPN user list.

Specify the Client-to-Gateway VPN Connection

Enter a pre-shared key to be used for the Phase 1 IKEv1 negotiation.

To specify the VPN connection:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > VPN**.

5. In the Remote Client to GW VPN Configuration section, click the **Edit** button next to the Pre-Shared Key field.

6. Type the pre-shared key.

   Note: The key is an alphanumeric string with a maximum length of 32 characters.

7. Verify that the VPN remote virtual IP and Mask fields have the correct values.

   Note: By default, these fields show the IP address and subnet mask for this gateway. This is how the remote clients will access this gateway.

8. Click the **Save** button.

To change the PSK for a remote client:

1. Click **Settings > General > VPN**.

2. In the Remote Client to GW VPN Configuration section, click the **Edit** button next to the Pre-Shared Key field.

3. Enter the new value

4. Click the **Save** button.

The new pre-shared key is saved.

Enable the Client-to-Gateway VPN

Enabling the VPN activates the remote client-to-gateway VPN server feature on the gateway. If you disable the VPN, your settings are retained.

To enable the VPN:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > VPN**.

5. Select the VPN Status **Enable** radio button.

6. Click the **Apply** button.

The VPN connection is activated.

To disable the VPN:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > VPN**.

5. Select the VPN Status **Disable** radio button.

6. Click the **Apply** button.

The VPN connection is disabled, but your VPN settings are retained.

Configure a Windows Computer as a Remote Client

This example describes how to use NETGEAR ProSAFE VPN client software to set up a VPN client for the gateway.

To use NETGEAR ProSAFE to set up a VPN client:

Download the trial version of NETGEAR ProSAFE VPN client (VPNG01L/VPNG05L Professional Software Version 5.14.003) and install it on the Windows computer.

1. This software is available here: http://kb.netgear.com/app/answers/detail/a_id/20316.

2. Launch the VPN client software.

3. In the left pane, select **Global Parameters**.

4. Specify the following settings:

   - Lifetime (sec):

     - Authentication (IKE): Enter **3600**, **360**, **28800**.

     - Encryption (IPSec): Enter **3600**, **300**, **28800**.

   - Dead Peer Detection (DPD):

     - Check interval: Enter **30**.

     - Max. number of retries: Enter **5**.

     - Delay between retries: Enter **15**.

   - Miscellaneous:

     - Retransmissions: Enter **2**.

     - X-Auth timeout: Enter **60**.

5. In the left pane, select **Gateway**, and click the **Authentication** tab.

6. In the Authentication screen, specify these settings:

   - In the Addresses section, specify the following:

     - In the **Remote Gateway** field, enter the WAN IP address.

     - Select the **Pre-Shared Key** radio button and enter the same key that is configured on the gateway.

   - In the IKE section, specify the following:

     - Encryption: Select **3DES**.

- Authentication: **Select SHA-1**.

- Key Group: Select **DH2 (1024)**.

7. Click the **Advanced** tab.

8. Specify these settings in the Advanced screen:

   - In the Advanced Features section, select the Mode Config check box and leave the other settings as shown.

   - In the X-Auth section, specify how the client user enters credentials:

     - To enable a pop-up, select the **X-Auth Popup** check box.
       With this setting, the client opens a pop-up window prompting the user to enter the user name and password.

     - To avoid using a pop-up, clear the **X-Auth Popup** check box and type the user name and password in the Login and Password fields.

   - Leave the Local ID field and Remote ID field blank.

9. Under the Gateway heading, select **Tunnel**, and click the **IPSec** tab.

10. Specify these settings on the IPSec screen:

    - In the Address type list, select **Subnet Address**.

    - In the Remote LAN address and Subnet mask fields, enter the gateway IP address and subnet mask.

      Note: The gateway and the client's network must have different subnet ranges that do not overlap.

    - In the ESP section, specify the following:

      - Encryption. Select **3DES**.

      - Authentication. Select **SHA-1**.

      - Mode. Select **Tunnel**.

    - In the PFS section, specify the following:

      - Select the **PFS** check box.

      - In the Group list, select **DH2(1024)**.

11. Leave the rest of the tabs with their default values.

12. Click the **Apply** button.

13. Click the **Save** button.

14. To initiate the VPN connection to the gateway, right-click the tunnel on the left pane and select **Open Tunnel**.

When the connection is initiated, the icon on the Tunnel menu on the left pane turns green to indicate that the tunnel is established.

The remote client device can access the LAN-side resources of the gateway including access to the gateway web management interface.

Configure a Mac Computer as a Remote Client

This example uses the IP Securitas VPN client software.

To configure a Mac computer as a remote client:

1. Download the trial version of IP Securitas VPN client and install it on the Mac computer.

   IPSecuritas VPN client Version 3.4 for MAC OS platforms from Lobotomo Software is available here: http://www.lobotomo.com/products/IPSecuritas/
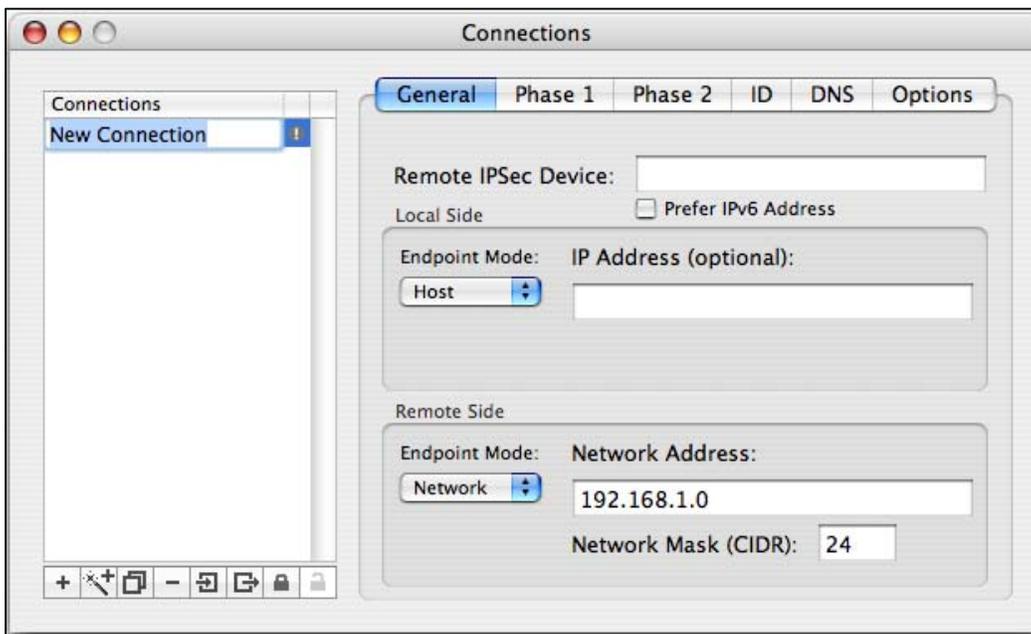
2. Launch the VPN client software.

3. Click **Connections > Edit Connections**.
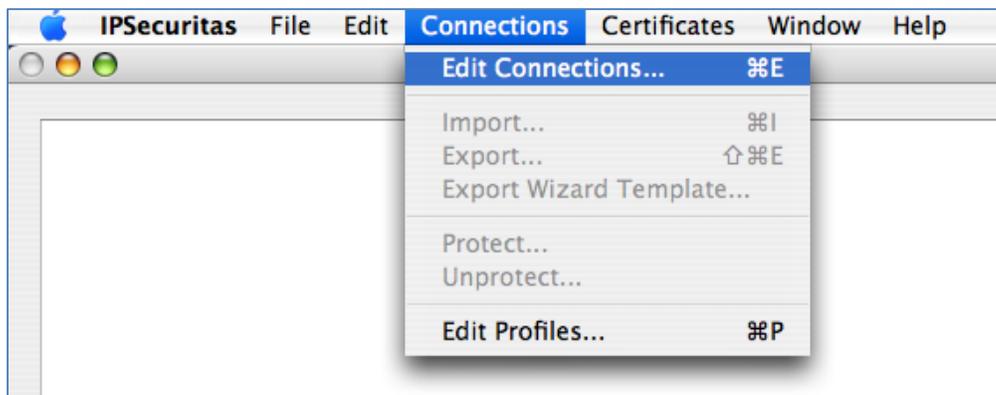
4. In the Connections pane, click the **+** (plus) icon in the lower left corner.
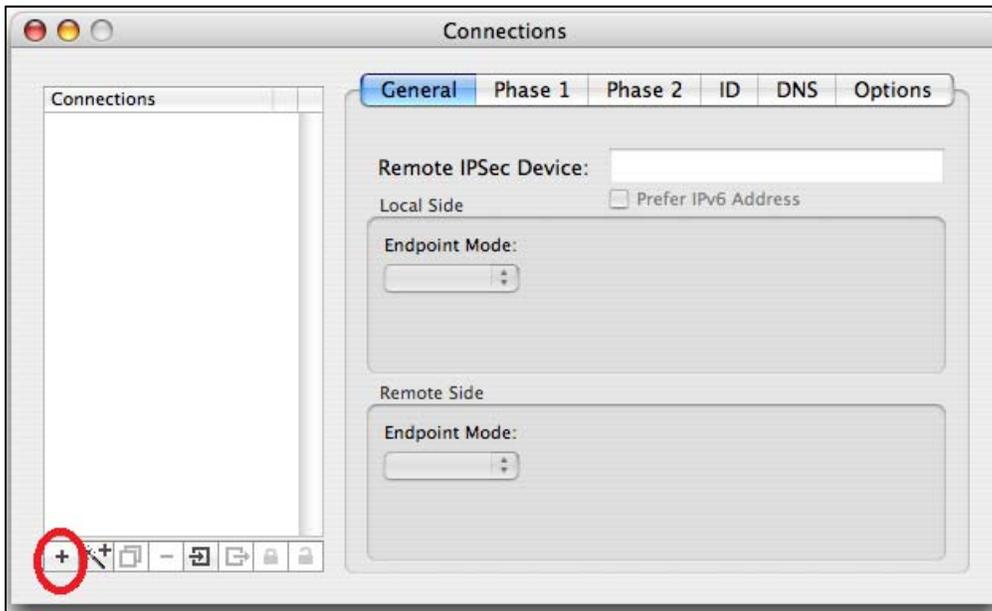
5. Enter a connection name that is easy to understand.

6. Click the **General** tab.

7. Specify the following:

   ▪ In the Remote IPSec Device field, enter the WAN IP address of the gateway.

- In the Remote Side section, enter the LAN-side IP subnet of the gateway with the subnet mask in CIDR format.

The gateway and the client's network must have different subnet ranges that do not overlap.

8. Click the **Phase 1** tab.

9. Specify the following:

   - Lifetime: Enter **1800** and select **Seconds**.

   - DH Group: Select **1024 (2)**.

   - Encryption: Select **3DES**.

   - Authentication: Select **SHA-1**.

   - Exchange Mode: Select **Main**.

   - Proposal Check: Select **Obey**.

   - Nonce Size: Enter **16**.

10. Click the **Phase** 2 tab.

11. Specify the following:

    - Lifetime: Enter **1800** and select **Seconds**.

    - PFS Group: Select **1024 (2)**.

    - Encryption: Select the **DES**, **3DES**, **AES 2256**, **AES 192**, and **AES 128** check boxes.

    - Authentication: Select the **HMAC MDS** and **HMAC SHA-1** check boxes.

12. Click the **ID** tab.

13. Specify the following:

    - Leave the Local Identifier and Remote Identifier fields set to **Address**.

    - Select **XAuth PSK** in the Authentication Method section and type the pre-shared key, user name, and password that you specified in the gateway.

14. Click the **Options** tab.

15. Specify the following:

- Select these check boxes:

   - **IPSec DOI**

- **SIT_IDENTITY_ONLY**

- **Initial Contact**

- **Enable MODE_CFG**

- **Request Certificate**

- **Send Certificate**

- **Unique SAs**

- **IKE Fragmentation**

- Leave NAT-T set to **Disable** and the Action after connection timeout set to **Give up**.

16. Close the Edit Connection window. The settings are saved.

17. In the main screen, highlight the connection name and select **Start**.

Once the connection is established, the icon to the right of the connection name turns green. The client computer can access the LAN-side resources of the gateway including the web management interface of the gateway.

Set Up a Site-to-Site VPN

This example describes how to set up a site-to-site VPN tunnel between two gateways at different locations. The LAN subnets of these two gateways must each be in a unique range.

To do this, you must complete the following tasks:

1. Make sure that each gateway uses a different subnet range and that the ranges do not overlap.

2. Specify the VPN connection for each gateway.

3. Enable the VPN on each gateway.

Specify the Site-to-Site VPN Connection

To specify the VPN connection information:

1. On the first gateway, select **Settings > General > VPN**.

2. In the Site-to-Site VPN configuration section, click the **Edit** button next to the Pre-Shared Key (PSK) field.

3. Type a unique pre-shared key.

   Note: The key is an alphanumeric string with a maximum length of 32 characters.

Note: This pre-shared key is unique to the site-to-site VPN configuration. If you set up a client-to-gateway VPN tunnel with this gateway, you must use a different pre-shared key for the site-to-site VPN.

4. In the Site-to-Site Configuration Details section, click the **Add** button.

5. In the Site Name field, type a meaningful name that is easy to understand.

6. In the WAN IP field, enter the remote gateway's WAN IP address.

7. In the Remote Site IP address and Subnet field, enter these settings from the remote gateway.

    Note: Each gateway must have a unique non-overlapping IP address range.

8. Click the **Save** button.

9. For the second gateway, repeat Steps 1–8 of this procedure.

Enable the Site-to-Site VPN

Enabling the VPN activates the VPN server feature on the gateway.

To enable the VPN:

1. On the first gateway, select **Settings > General > VPN**.

2. Select the VPN Status **Enable** radio button.

3. Click the **Apply** button. The VPN connection is activated.

4. On the second gateway, select **Settings > General > VPN**.

5. Select the VPN Status **Enable** radio button.

6. Click the **Apply** button. The VPN connection is activated.

The IPSec VPN tunnel is established between the two gateways. The LAN-side resources from one gateway can access the other through this tunnel.

To disable the VPN:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > General > VPN**.

5. Select the VPN Status **Disable** radio button.

6. Click the **Apply** button.

The VPN connection is disabled, but your VPN settings are retained.

Frequently Asked Questions

Find out answers to questions you may have.

How Can I Tell I'm Connected to 3G or LTE?

When you log in to the gateway (http://myrouter), the network type icon (3G or LTE) appears in the Status section on the left side of the page, and the connection status is shown on the Network > Status Details Page.

How Do I Connect to Wi-Fi?

You may have to manually connect to Wi-Fi after certain events — for example, as part of the initial device setup, or after a software update.

Tip: The Wi-Fi network name and password are displayed on the label of the gateway.

Tip: Alternatively, you can use WPS to connect a device to the gateway, if your device supports WPS. (See Connecting Through WPS.)

To connect to Wi-Fi:

7. Do one of the following, depending on your operating system.

   ▪ Windows 7: Right-click the Wi-Fi icon in the system tray.

   ▪ Windows Vista: Click **Control Panel > Network and Internet > Network and Sharing Center > Connect to a network**.

   ▪ Windows XP: Click **Control Panel > Network Connections > Wireless Network Connections > View available wireless networks**.

   ▪ Mac: Click the AirPort icon (in the upper right corner of your screen).

   ▪ Linux: Please see the user documentation of the Linux distribution.

   ▪ Other operating systems: Please see the user documentation for your operating system or computer.

8. Select one of the Wi-Fi networks provided by the gateway and connect to it. (If prompted for a network key/security key/password, enter the Wi-Fi password.)

Is Roaming on LTE Supported?

At the time of this release, roaming (that is, using a network other than Sprint) on LTE is not supported.

To change the roaming setting, see Setting the Roaming Mode.

What Do I Do if I Forget the Main or Guest Wi-Fi Password?

To see the Main Wi-Fi password and Guest Wi-Fi password:

1. Look on the gateway's label.

2. If you changed the Wi-Fi password and have forgotten what it is, use an Ethernet cable to connect a computer to one of the gateway's yellow Ethernet LAN ports.

3. On a computer or wireless device that is connected to your gateway, launch a Web browser.

4. In the address or URL field of your browser, type **http://myrouter**.

5. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

6. Click **Wi-Fi > Options**.

What Do I Do if I Forget the Administrator (admin) Password?

The default password is password. If you changed the password and enabled password recovery, you can recover your password.

To recover a forgotten administrator (admin) password:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**

3. When you are prompted to login, click **Cancel**.

   Note: If password recovery is enabled, you are prompted to answer two security questions.

4. Enter the saved answers to the security questions.

5. Enter the serial number of your router.

   Note: The serial number is on the gateway's label.

If you forgot the administrator password and you did not enable password, you will need to contact Sprint Customer Support for assistance with resetting the software to default settings. (See Resetting to Factory Default Settings.)

If the Connection is "Always On," Am I Always Being Billed?

No. The connection to the network goes dormant after a period of inactivity, but the connection can be re-established faster than having to reconnect. Billing occurs only when data is passed across the network.

Questions About GPS

Find answers to common questions about GPS.

What is GPS?

GPS stands for Global Positioning System, which is a system that uses a series of 24 geosynchronous satellites to provide location data.

GPS satellites transmit signals to equipment on the ground. GPS receivers passively receive satellite signals, but do not transmit.

Where Can I Use GPS?

GPS works wherever you have line-of-sight access to the GPS satellites.

How Do I Enable or Disable GPS?

By default, GPS is disabled. To enable GPS, see Enabling / Disabling GPS.

What are some GPS Limitations?

Weather conditions or tall nearby buildings may affect your ability to get a clear view of the satellites and thus to acquire a GPS fix.

How Can I Stream GPS Data to Use With a Third-party GPS Application?

GPS NMEA data is streamed over Wi-Fi or over a tethered USB connection using a virtual COM port.

To stream NMEA data for a third party GPS application:

1. Set GPS Mode to **Continuous**. (See Setting the GPS Mode.)

2. Determine the COM port number that your NETGEAR device (that is, your NETGEAR 6100D) is using.
   In the following example for Windows, the Device Manager shows that COM 16 is used.

In your case, the COM port number might be different.

> **Note:** If you don't know how to access the Device Manager, see
> http://kb.netgear.com/app/answers/detail/a_id/22868.)

3. Configure your GPS application to use the same COM port. For help, see the
   documentation of the GPS application.

Questions About WPS

Find answers to common questions about WPS.

What is WPS?

Wi-Fi Protected Setup (WPS) provides a fast, simple, and secure way to connect WPS-enabled devices to your Wi-Fi network. You don't have to give the name (SSID) and Wi-Fi password of your network to other users.

The WPS feature is available on certain cameras, printers, smartphones, and laptops. These devices have either a hardware button or a WPS-related option in the software. Please consult the user documentation of your device.

How do I Use WPS?

Please see Connecting Through WPS.

If a Wireless Device has a WPS Button or a WPS Software Option, Must I Use it to Connect Via Wi-Fi?

If this is the only way your device provides to connect through Wi-Fi, then you must use the WPS button or the WPS software option. Some laptops support two methods — a WPS button or software option, and Wi-Fi network manager software where you can connect by entering the Wi-Fi network name (SSID) and password, as described in How Do I Connect to Wi-Fi?.

Please consult the user documentation of your device.

How Do I Access My Corporate Network Through a VPN?

Once you complete a wireless connection, you may need to launch an extranet client provided by your company and supply the appropriate user name and password to gain access. For support, contact your company help desk.

Are Terminal Sessions Supported?

Terminal sessions (for example, via telnet or ssh) are not supported.

Tips

This section provides information on getting the most out of your device and your network connection.

Gateway Location

Follow these guidelines in placing your device.

- Avoid moisture or extreme temperatures.

- For improved reception, place your gateway near a closed window.

- Place your device within easy reach of a reliable power supply and the computer to which it will be connected.

Improving Signal Strength

There are several ways you can improve the signal strength.

- Make sure you're inside a network coverage area.

- Try reorienting your device.

- Move your device and your computer to another location — you may be in or near a structure that is blocking the signal. Every obstacle (for example, walls, ceilings, furniture) between the gateway and other wireless devices decreases the signal strength.

- Place your gateway in a centralized location, as high as possible in the room.

- Make sure there's plenty of space around your gateway to provide the best signal reception.

- Keep your gateway at least 3–6 feet away from electrical devices that generate RF interference (for example, microwaves, TVs, 2.4 GHz cordless phones, cellular phones, baby monitors, wireless speakers). If you're not using these electrical devices, turn them off.

- If possible, place your gateway and your computers and devices so that the signal passes through open doorways or drywall, as opposed to concrete, brick, metal, walls with insulation, and so on.

- If you cannot obtain service, contact Sprint — a network or account problem may be preventing you from obtaining service.

Improving 3G Network Service

To improve your network service, periodically check for PRL and profile updates.

The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem.

To check for these updates:

1. On a computer or wireless device that is connected to your gateway, launch a Web browser.

2. In the address or URL field of your browser, type **http://myrouter**.

3. When prompted to log in, enter **admin** for the user name and type the password. (The default password is **password**.)

4. Click **Settings > Network > Preferences**.

5. Click **Update PRL**.

Improving Wi-Fi Performance

There are several ways you can improve Wi-Fi performance.

- Try a different channel number. (See Wi-Fi Channel.)

- Check whether any device updates are available. (See Update Software and Firmware.)

- See the tips in Improving Signal Strength.

Windows XP and Windows 7 Users

1. Open the Device Manager.

    In Windows XP:

    - Click **Start > Settings > Control Panel**.

    - Double-click **System**.

    - Click **Hardware**.

    - Click **Device Manager**.

    In Windows 7:

    - Click **Start > Control Panel**.

    - Click **Device Manager**.

2. Double-click **Network adapters**.

3. Double-click the Wi-Fi client network adapter of your computer — for example, "Intel(R) WiFi Link 5100 AGN" in the screenshot below.
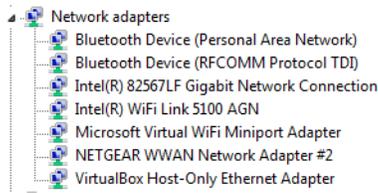
4. If the Wi-Fi client network adapter is by Intel, click **Advanced** and, in the **Property** list, click **Power Management** and move the slider all the way to the right (to **Highest**). Click **OK**.

— or —

If the Wi-Fi client network adapter is not by Intel, select a configuration with minimal power savings (to maximize throughput).

Note: The above settings are often controlled by 3rd-party value-add applications and may be automatically changed. If Wi-Fi performance improves for a while after performing the above steps, but then declines, recheck the above settings.

Security Tips

Follow these tips to minimize security risks.

- Change the Wi-Fi network name (SSID) and Wi-Fi password on a regular basis. (See Change Wi-Fi Network Names and Passwords.)

- Disable SSID Broadcast. (See Options Section.)

- Use the highest level of Wi-Fi security that your devices support. (See Wi-Fi Security.)

- Change the login password. (See Changing the Password.)

- Use MAC filtering to specify computers that are or aren't allowed to connect to the network. (See Allowing or Denying Computers Access to the Network (MAC Filter).)

Finding the MAC Address

You'll need to know the MAC address of a device in a couple of cases.

- Allowing or denying computers access to the network. (See Allowing or Denying Computers Access to the Network.)

Tip: You can display a list of connected devices, including the MAC address of each device. See Displaying and Blocking Currently Connected Devices (Block List).

The steps to finding the MAC address of a device vary, depending on your operating system.

Windows

1. Open a command prompt window.

   ▪ Click **Start** and **Run**.

   ▪ Type **cmd** or **command**, and click **OK**.

2. At the command prompt, type **ipconfig/all** and press **Enter**.

3. Write down the Physical Address for the entry that relates to the wireless network connection; it appears as a series of numbers and letters — this is the MAC address of your wireless adapter.

Mac OS X

1. From the Apple menu, select **System Preferences**.

2. Select **Network**.

3. Select the adapter that is connecting to the routing hardware.

4. Select **Advanced**.

5. Select **Ethernet**. The Ethernet ID is listed. This is the same as the MAC address.

Linux

Please see the user documentation of the Linux distribution.

Other Operating Systems

Please see the user documentation for your operating system or computer.

Finding the IP Address

You'll need to know the IP address of a device when configuring certain features.

● Port forwarding

● DMZ

The steps to finding the IP address of a device vary, depending on your operating system.

Windows

1. Open a command prompt window.

2. Type **cmd** or **command**, and click **OK**.

3. At the command prompt, type **ipconfig** and press **Enter**.

4. Write down the IP Address for the entry that relates to the wireless network connection. (The IP address might be listed under "Ipv4 Address," or something similar.)

Mac OS X

1. From the Apple menu, select **System Preferences**.

2. Select **Network**.

3. Select the wireless adapter. The IP address is displayed in the right pane.

Other Operating Systems

Please see the user documentation for your operating system or computer

Troubleshooting

Learn about various troubleshooting tips, and what to do when a specific message is displayed.

General Tips

Here are some general tips to get you started.

- If some settings are preventing you from connecting to Wi-Fi, connect via Ethernet. Cable your computer to an Ethernet LAN port on your device.

- Go to sprint.com/support to access troubleshooting and other resources.

- The knowledge base at the NETGEAR website (support.netgear.com) may also be useful.

Insufficient Signal Strength

If you have insufficient signal strength, an icon is displayed on your device's home screen, and on the web page's Connection Details section.

Insufficient signal strength, indicated by 🚫, may occur because:

- You are outside network coverage areas.

- Your device's internal antenna is pointing in the wrong direction.

- You are in or near a structure that is blocking the signal.

- You are near a device that is causing radio signal interference.

- A network or account problem is preventing you from obtaining service.

See also Improving Signal Strength.

Cannot Connect to Wi-Fi

If your computer cannot connect to the Main or Guest Wi-Fi networks of the NETGEAR 6100D, there are several things you should check.

Make sure that:

- The maximum number of Wi-Fi devices has not been reached. (To determine the number of connected Wi-Fi devices and set the maximum, see Displaying and Blocking Currently Connected Devices (Block List) and Setting the Maximum Number of Wi-Fi Devices.)

- You're connecting to the correct Wi-Fi network (SSID), and you're using the correct Wi-Fi password.

- Nobody has changed the name or password of the Wi-Fi network.

- Your computer supports the type of Wi-Fi security that the network is set to use.

Note: To connect to the gateway's Wi-Fi network, each computer or Wi-Fi device must support the gateway's Wi-Fi security type.

- Your computer supports Wi-Fi 802.11g (if **Connection Rate** is set, in the Wi-Fi Options Section to **802.11g only**).

- Your computer has not been blocked through MAC filtering. (See Allowing or Denying Computers Access to the Network (MAC Filter).)

Cannot Display the Home Page

Your Web browser may display an error message when you try to display the home page. The error message depends on your Web browser.

- "Could not connect to remote server" (Opera)

- "Internet Explorer cannot display the webpage" (Internet Explorer)

- "Oops! This link appears to be broken" (Google Chrome)

- "Safari can't open the page" (Safari)

- "The connection has timed out" (FireFox)

Check the following:

- Your gateway is turned on. (See Turning Your Device On and Off.)

- You have established a connection to your device (through Wi-Fi or through an Ethernet cable).

- Make sure that you're typing the correct address in the Web browser.

  - Try **http://myrouter** (unless you've changed the URL in Changing the URL.)

  - If the home page is still not displayed, try **http://192.168.0.1** or, if you're using custom routing settings, replace "192.168.0.1" with the appropriate IP address.

- The Web browser is a recent version, and Java-enabled. The following are recommended:

  - Internet Explorer 10.0 or Higher

  - Firefox 21.0

- Google Chrome (version 30 or higher)

- If your computer has other adapters (for example, Ethernet) connected to other networks, disable or remove them from your computer.

- If Internet security software is running on your computer, disable it and see whether the error message still occurs. Some firewall software may block access to the home page.

- If DHCP is enabled on your device, make sure DHCP is enabled on your computer. (See DHCP.)

- Check your Web browser settings:

1. Open the Control Panel in Windows.

2. Double-click **Internet Options**.

3. From the **Security** tab, restore the default settings.

4. From the **Connections** tab, select **Never dial a connection**.

5. From the **Advanced** tab, restore the default settings.

6. Close and reopen your Web browser.

- Disconnect your device from your computer (if you're using the micro-USB cable). Remove the battery from your device. Reinsert the battery.

If, after checking all of the above, you still cannot display the home page, consider resetting the software to default settings. (See Resetting to Factory Default Settings.)

Cannot Connect to the Mobile Broadband Network

If this message is displayed, go through the following steps.

- Make sure your computer is connected to your device (through Wi-Fi or with an Ethernet cable). (See How Do I Connect to Wi-Fi? or Connecting with Ethernet.)

- Make sure you're in a network coverage area.

- Check the **Network Mode** setting (See Setting the Allowed Network Mode). For example, if it's set to **LTE Only**, you won't be able to connect if you don't have LTE coverage.

- If you're roaming on 3G, make sure that roaming is enabled. (See Setting the Roaming Mode.) (Roaming is not supported on LTE.)

Note: Roaming charges may apply.

- If you're roaming internationally, make sure that **Any Network** is selected. (See Setting the Roaming Mode.)

- Try the tips in Improving Signal Strength.

- Check with Sprint — a network or account problem may be preventing your device from obtaining service.

GPS Doesn't Seem to Be Available

Make sure that GPS is enabled. (See Enabling / Disabling GPS.)

For best results, minimize the number of obstructions between your device and the GPS satellites.

Cannot Check for Updates

Make sure your device is connected to the AC charger or computer through the micro-USB cable.

Technical Specifications

This section lists the electrical, radio frequency, and other parameters of your device for those who require technical information.

Radio Frequency and Electrical Specifications

This section lists the radio frequency and electrical parameters of your device.

Item	Description
Approvals	FCC

Current	Maximum: ~900 mA
	Standby current:
	   - 4 mA (1xEV-DO/IS2000 hybrid mode)
	   - ~6.5 mA (LTE)

Transmit	PCS: 1850-1910 MHz
	Cellular: 824-849 MHz
	Secondary 800 MHz: 817-824 MHz
	LTE:
	   - Band 25: 1850-1915 MHz
	   - Band 26: 814-849 MHz
	   - Band 41 (TDD): 2496-2690 MHz
	UMTS/HSPA+:
	   - Band 1: 1920-1980 MHz
	   - Band 2: 1850-1910 MHz
	   - Band 5: 824-849 MHz
	   - Band 8: 880-915 MHz

Receive	PCS: 1930-1990 MHz
	Cellular: 869-894 MHz
	Secondary 800 MHz: 862-869 MHz
	LTE:
	   - Band 25: 1930-1995 MHz
	   - Band 26: 859-894 MHz
	   - Band 41 (TDD): 2496-2690 MHz
	UMTS/HSPA+:
	   - Band 1: 2110-2170 MHz
	   - Band 2: 1930-1990 MHz
	   - Band 5: 869-894 MHz
	   - Band 8: 925-960 MHz
	GPS: 1575.42 MHz

Software Specifications

This section lists the specifications that your device supports.

Item	Description
CDMA (3G) specification	IS-2000 Release 0
Data service	IS-707A
3GPP	Release 9
Wi-Fi specification	IEEE 802.11b IEEE 802.11g IEEE 802.11n
Wi-Fi security and encryption protocols	WEP Open & Shared WEP-64 WEP-128 WPA-Personal TKIP & AES (Pre-Shared Key or WPA-PSK) WPA2-Personal TKIP & AES (WPA2-PSK) WPA+WPA2-Personal (WPA+WPA2 PSK)
WPS	Wi-Fi Simple Configuration 2.0 (WSC 2.0) based Wi-Fi Protected Setup (WPS)
SMS (IS-637)	Not supported
FAX	Not supported
IOTA	Supported
OTASP (IS-683A, IS-683B, IS-683C)	Supported
OTAPA	Supported
PRL (Preferred Roaming List)	Supported
Authentication	Supported
Voice	Not supported
NAM	Single
Position Location	Standalone
TTY/Accessibility	Not supported
Mobile IP	Supported
Network protocols (routing hardware)	TCP, UDP, ARP, RARP, ICMP
VPN	Pass-through of the following VPN types: PPTP IPSec Tunneling of multiple VPN sessions simultaneously is supported.

Environmental Specifications

This section describes the environmental conditions that your gateway can be used in.

Item	Description
Operating temperature	32 to 140°F
Storage temperature	14 to +140°F
Humidity	149°F, 90% relative humidity for 24 hours

Mechanical Specifications

This section describes the dimensions and physical features of your device.

Item	Description
Dimensions (W x L x H)	2.72" x 4.33" x 0.61"
Weight	3.70 oz.
Headset jack	Not supported
LED	Blue / Amber / Orange

Wall Mounting

You can wall-mount your gateway.

To wall-mount the gateway:

1. Drill holes in the wall where you will wall-mount the gateway.
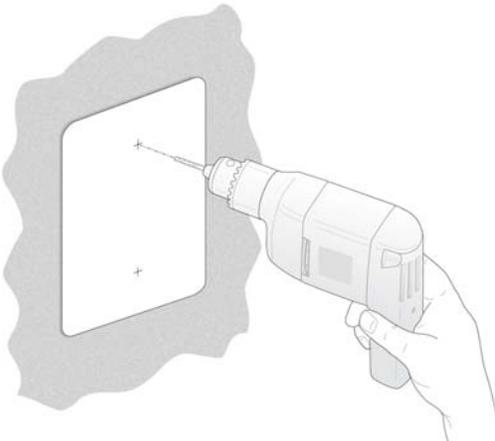
2. Install wall anchors in the holes.
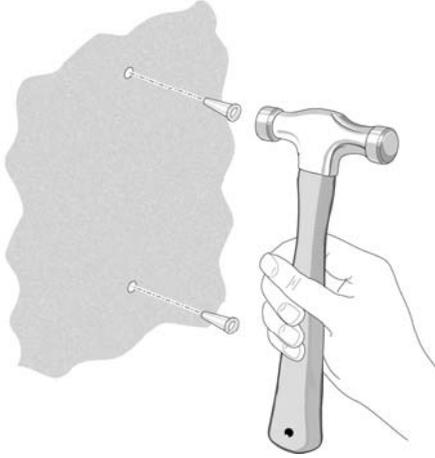
Note: Use pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or #6 type screw, 1 inch long (U.S.).

3. Insert screws into the wall anchors, leaving 3/16 in. (0.5 cm) of each screw exposed.

Safety Information

Read important safety information about your device.

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the NETGEAR 6100D are used in a normal manner with a well-constructed network, your device should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. NETGEAR accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using your device, or for failure of your device to transmit or receive such data.

Safety and Hazards

Do not operate your device under the following conditions.

- In areas where blasting is in progress

- Where explosive atmospheres may be present

- Near medical equipment

- Near life support equipment, or any equipment that may be susceptible to any form of radio interference.

In such areas, your device MUST BE POWERED OFF. Your device can transmit signals that could interfere with this equipment.

Do not operate your device in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, your device MUST BE POWERED OFF. When operating, your device can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Your device may be used at this time.

The driver or operator of any vehicle should not operate the device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some jurisdictions, operating such communications devices while in control of a vehicle is an offense.

Regulatory Notices

This section contains regulatory information for your device.

The design of the NETGEAR 6100D complies with U.S. Federal Communications Commission (FCC) guidelines respecting safety levels of radio frequency (RF) exposure for mobile devices, which in turn are consistent with the following safety standards previously set by U.S. and international standards bodies:

- ANSI / IEEE C95.1-1999, **IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3kHz to 300 GHz**

- National Council on Radiation Protection and Measurements (NCRP) Report 86, 1986, **Biological Effects and Exposure Criteria for Radio Frequency Electromagnetic Fields**

- International Commission on Non-Ionising Radiation Protection (ICNIRP) 1998, **Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)**

FCC ID: PY313200235

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

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

Country Code selection feature to be disabled for products marketed to the US/CANADA

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

WARNING (EMI) - United States FCC Information - This equipment has been tested and found to comply with the limits for a Class B computing device peripheral, 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: Any changes or modifications not expressly approved by NETGEAR could void the user's authority to operate the equipment.

This device complies with Parts 15, 24, and 27 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Legal

This section contains important license and legal information.

Patents

This product contains technology developed by or for NETGEAR, Inc.

This product includes technology licensed from QUALCOMM®.

Licenses

A large amount of the source code to this product is available under various free and open source licenses. Most is available under one or more versions of the GNU General Public License and/or GNU Limited General Public License.

The remainder of the open source software which is not under the GPL is available under one of a variety of more permissive licenses. Those that require reproduction of the license text in the distribution are listed in the sections that follow (starting with fontconfig License).

GNU General Public License (Version 2)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU General Public License (Version 3)

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the

work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for

software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not

apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These

actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will

continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

GNU Lesser General Public License (Version 2.1)

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copiesof this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.
The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has

appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License (Version 3)

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing

the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public

License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

License

Copyright © 2001 Keith Packard

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Keith Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Keith Packard makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

THE AUTHOR(S) DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 2002-2003 by Juliusz Chroboczek

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

libxml2 License

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

hash.c License

hash.c: chained hash tables

Reference: Your favorite introductory book on algorithms

Copyright (C) 2000 Bjorn Reese and Daniel Veillard.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHORS AND CONTRIBUTORS ACCEPT NO RESPONSIBILITY IN ANY CONCEIVABLE MANNER.

Author: breese@users.sourceforge.net

list.c License

list.c: lists handling implementation

Copyright (C) 2000 Gary Pennington and Daniel Veillard.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHORS AND CONTRIBUTORS ACCEPT NO RESPONSIBILITY IN ANY CONCEIVABLE MANNER.

Author: Gary.Pennington@uk.sun.com

trio.c License

Copyright (C) 1998 Bjorn Reese and Daniel Stenberg.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHORS AND CONTRIBUTORS ACCEPT NO RESPONSIBILITY IN ANY CONCEIVABLE MANNER.

locapi License

Copyright (c) 2009, QUALCOMM USA, INC.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the QUALCOMM USA, INC. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

pimd License

Copyright (c) 1998-2001

University of Southern California/Information Sciences Institute.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part of this program has been derived from mrouted.

The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

shadow License

Copyright (c) 1989 - 1994, Julianne Frances Haugh

Copyright (c) 1996 - 2000, Marek Michałkiewicz

Copyright (c) 2001 - 2006, Tomasz Kłoczko

Copyright (c) 2007 - 2009, Nicolas François

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

    2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

    3. The name of the copyright holders or contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ISC License

Copyright 2004-2010 by Internet Systems Consortium, Inc. ("ISC")

Copyright 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. I.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Trademarks

SPRINT and the logo are trademarks of Sprint.

NETGEAR and the NETGEAR logo are trademarks of NETGEAR, Inc.

Windows® is a registered trademark of Microsoft Corporation.

Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Wi-Fi, WPA, and WPA2 are registered marks of the Wi-Fi Alliance.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated.

Other trademarks are the property of the respective owners.

Copyright

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of NETGEAR, Inc. NETGEAR AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY NETGEAR PRODUCT, EVEN IF NETGEAR AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall NETGEAR and/or its affiliates aggregate liability arising under or in connection with the NETGEAR product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the NETGEAR product.

Additional Information and Updates

For up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases, visit netgear.com.

Index