WIFIRANGER™

A WINEGARD® COMPANY

USER GUIDE

FIRMWARE 7.1.0b11

WWW.WIFIRANGER.COM

TABLE OF CONTENTS

1 INTRODUCTION

Your WiFiRanger router is designed to be the communications hub for your RV, yacht, or over-the-road truck. The first sections of this guide are focused on getting you familiar with the basic features of the Ranger so you can be connected to the internet as quickly as possible. The later sections provide detailed discussions of the multitude of advanced features embedded in every Ranger.

Although WiFiRanger currently makes and markets nearly a dozen different types of routers, all of them use the same embedded software which we will refer to as the firmware. Regardless of the specific model of Ranger that you have, this guide will be applicable to it.

All WiFiRanger routers are controlled though an embedded Control Panel which is accessed through the browser of whatever web-enabled device you choose to use. Regardless of whether you have a laptop, an iPad, a smartphone, or a desktop computer, it will access your Ranger through the Ranger's control panel in the same manner.

Note: By default, all Rangers are delivered with certain advanced features hidden from users who may not need to access them. Hiding advanced features is controlled by a "switch" on the Setup tab of the Ranger's control panel. For simplicity this guide has been prepared with "Hide Advanced Features" being set to "off." If your control panel doesn't resemble the one pictured in this guide it may be because you have Hide Advanced Features set to "ON". There is no risk to setting Hide Advanced Features to "OFF"; displaying them doesn't result in any changes being made to your Ranger.

All WiFiRanger routers have the ability to connect to distant WiFi sources (up to several miles away depending on the Ranger model) and can rebroadcast signals from those WiFi sources inside your RV, boat or truck. That's a fundamental feature of all Ranger router, and enhanced WiFi connectivity has been a key design objective for WiFiRanger routers for more than 10 years. The first section of this guide provides instructions for using the WiFi capability of your Ranger to connect to WiFi sources and, through them, to the internet.

In addition, many WiFiRangers currently being sold also have integrated cellular modems which enable them to connect to available cellular networks. Your Ranger may have such a modem already installed. If not, for several Ranger models it is possible to "field install" a modem as an after-market accessory. WiFiRanger Customer Support can tell you if it is possible to add a modem to your Ranger if it doesn't already have one installed. The second section of this guide provides instructions for connecting to a cellular network using a Ranger's integrated modem.

The remainder of the guide discusses the operation of each element of the WiFiRanger including advanced features, such as the use of MultiWAN connections. It is intended to serve as a reference guide to enable you to access the Ranger's advanced features as you feel comfortable doing so.

2 BASIC GUIDE TO CONNECTING TO WIFI ACCESS POINTS

Your WiFi Ranger may consist of a single router either on the roof of your vehicle or inside it, or it may be comprised of two routers, one on the roof and one inside. Both configurations are treated separately in this section of the guide.

2a SINGLE ROUTER RANGER SYSTEMS

Using your WiFiRanger to connect to the internet is a 3-step process.
Follow the steps below to get your WiFiRanger online:

STEP 1 Power up your WiFiRanger and connect your laptop, phone, or other device to its WiFi broadcast. The default WiFiRanger broadcast has the format "**Pvt.WFR_*Model.ABCD***" where *Model* identifies the type of WiFiRanger router and ABCD are 4 unique numbers (which also happen to be the last 4 digits in the WiFiRanger's ID number). The default password for this WiFi broadcast will be "**changemenow*ABCD***" where *ABCD* are the same 4 numbers. Connect to this broadcast the same way you would any other WiFi.

STEP 2 Open a browser window on your device and use the browser to access the address of the WiFiRanger's Control Panel. The Control Panel will be found at **http://mywifiranger.com/**. Please note that this isn't an internet address; it is a local address which your browser can access without being connected to the internet.

In order for your browser to be redirected to the control panel, it is essential that Control Panel Redirect (on the Setup page) be set to "ON". It should be set automatically to this state but, if you encounter any difficulties, you should verify that the setting has not been changed.

In addition, if you are connecting to the Ranger by using an Android phone, you may encounter a log-in screen which will prompt you to confirm that you want to connect to the Ranger. Doing so will take you to the control panel.

If you are using a smart phone to connect to the control panel, it may be advisable to disable cellular data to force the phone to use WiFi. Otherwise it may switch to cellular without you knowing it.

If, for some reason, you cannot access the control panel using the above link, the control panel can also be accessed at http://10.1AB.CD.1:8080/ where ABCD are the same 4 numbers referenced previously.

STEP 3 When you access the Control Panel, you will be presented with a list of all the WiFi networks that the WiFiRanger has identified arranged in decreasing order of signal strength. This is the Main page of the Ranger's control panel. Later sections of this guide will acquaint you with other features of this page, but for now simply find the WiFi network you wish to connect to and click on the word CONNECT at the left side of its line.

Enter its password (network key) if you are prompted to do so. Each time you click on the SCAN button at the top of the WiFi section of the Main page the Ranger will update its list of available broadcasts. Note that if you have moved to a new location your Ranger may display the broadcasts from its prior location until you click on SCAN. Note that some networks will be marked as Open and will not require a password to connect.

After the WiFiRanger connects to the desired WiFi network, all of your computers and other devices that are connected to the WiFiRanger's WiFi will now have internet access (assuming, of course, that the WiFi network the WiFiRanger is connected to has internet available).

That's all there is to getting connected. Of course, your Ranger has a lot more features that you may wish to learn about, but, for now, you are connected to the internet through your Ranger.

2b DUAL ROUTER RANGER SYSTEMS

Dual router Ranger systems utilize two routers operated through a single control panel to provide optimum WiFi performance. Having two separate routers allows the function of communicating with a WiFi access point to be separated from the function of communicating with your networked devices. This "decoupling" of functions allows the system's two radios to each be dedicated to a single function rather than acting in both roles. This provides a modest, but measurable, performance improvement.

[For the purposes of this Guide we're going to assume that your devices have been properly installed and are connected to each other via the power and Ethernet connectors of the Tetherpoint cable. If you have any questions about the installation of your routers, please refer to this guide: Converge Owner's Guide]

To connect to your dual router system, start by examining the list of available WiFi networks displayed on your computer, phone or other device. Depending on which indoor router you have you will see either one or two broadcasts (network SSIDs) from the inside Ranger probably labeled as 2GHz and 5GHz along with the model of the Ranger which could be Poplar, Spruce, Aspen or Core. There will also probably be another broadcast labeled with the model of the rooftop Ranger (Teton, Denali, Everest, or Sky). For purposes of this quick start guide we will focus on connecting to one of the broadcasts from the indoor router.

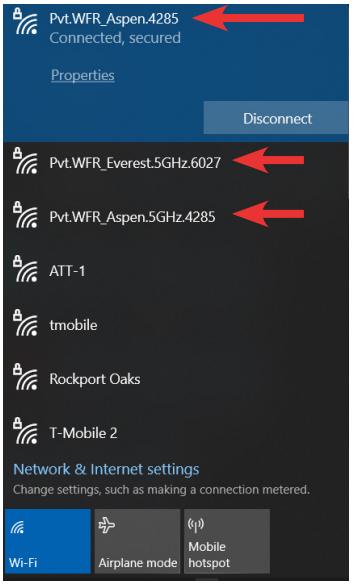

Figure 2b-1 shows three WiFi broadcasts from an Aspen/Everest WiFiRanger system; two broadcasts at 2.4 and 5 GHz from the Aspen and one 5GHz one from the rooftop Everest.

FIGURE 2b-1

Once you have selected the WiFi broadcast you wish to connect to, go to section 2a and follow the procedures for connecting to the WiFi and to the Ranger's control panel. When you have accessed the control panel return here.

You have now connected to the indoor router but to make full use of your two-router system you need to configure the rooftop router.

Go to the Control Panel and notice that there are tabs at the top of the control panel “box”. One of these tabs is labeled Setup. Click on that label and you will be taken to the Setup page. At the top of the page there are a series of lines, one of which is labeled “WFRControl [model type of your rooftop Ranger]”. That line might show in dark type, or it might be grayed out. Check to see if there is a “check” in the Active column of this line. If there isn’t one, then put one there now. Next, use the Save button at the bottom of the page to save what you have done.

Next click on the “settings” gear on the right side of the WFRControl line. A new window will open; at the top of this window, you should see the words “Controlling ABCDEF via Ethernet” where ABCDEF is the ID number of your rooftop router. If you don’t see those words, click on the Repair button. If that doesn’t result in the proper text appearing, consult the detailed WFRControl section of this guide. Figure 2b-2 shows an Everest rooftop system being controlled by an Aspen.

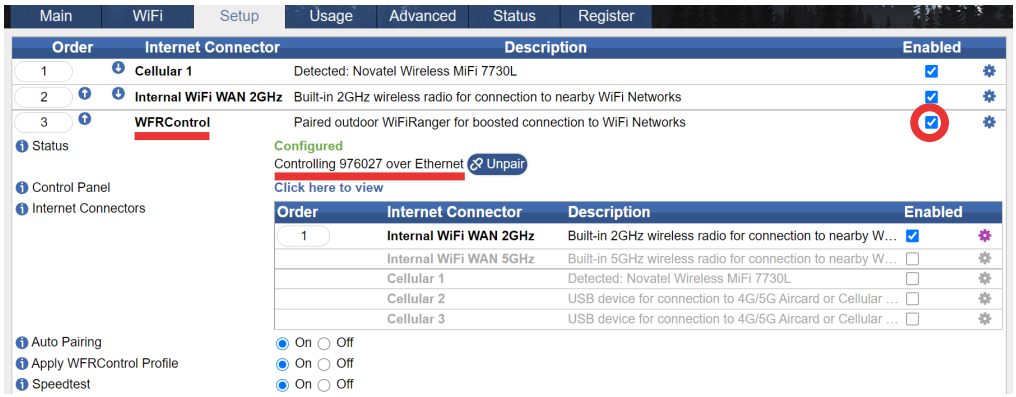

FIGURE 2b-2

If you have been successful in getting your two Ranger’s to “pair” you can now return to the Main page of the control panel. At the top left in the “WiFi box” you will now have a drop-down with the options being the Internal WiFi connections for your indoor router and for your rooftop router. The number of items displayed will depend on whether your Rangers are single band (2.4 GHz) or dual band (2.4 and 5 GHz) and whether you have activated all these options. Each time you change the dropdown selection and click on Scan, the Ranger will display the WiFi sources that the specified radio is seeing. Figure 2b-3 shows the dropdown box for the 2 and 5 GHz radios for an Aspen-Everest pair.

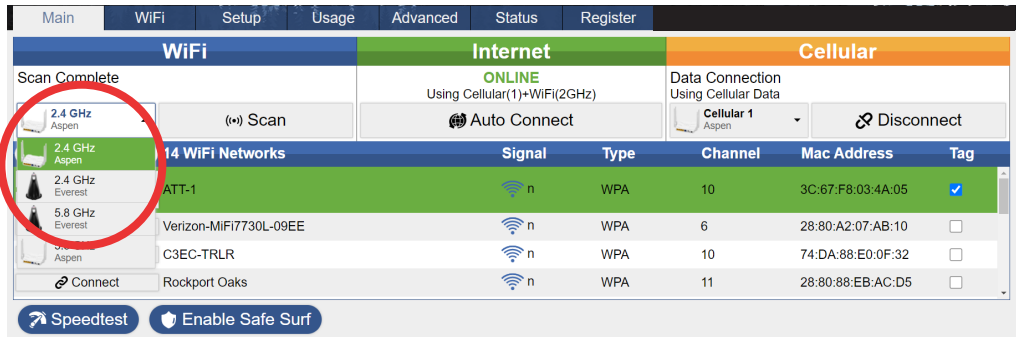

FIGURE 2b-3

2c USING THE CONTROL PANEL'S SETUP TAB TO SELECT INTERNET CONNECTIONS

The Setup tab is the functional heart of a Ranger's control panel; through it users decide what kinds of internet connections they wish to utilize. At the top of the Setup page is the list of internet connections that your specific model Ranger is capable of supporting. All Rangers are capable of supporting the same "set" of internet connections, but the specifics will vary depending on Ranger model. When you configure your system you will need to decide what set of internet connections you expect to use. You can change this set anytime you wish, but it is good practice not to activate connections that you have no intention of using.

Any internet connection in the list can be "enabled" by putting a check in the Enabled column of the corresponding line and then saving that action using the button at the bottom of the page. The title of the line will change from "grayed out" to bold when the line is activated.

In addition to simply enabling or disabling a connection, there are addtitional functions which can be accessed by clicking on the "gear" at the right side of each line. When the gear on an active line is clicked, a window will open. In that new window are controls for several additional functions related to that connection. The following are the functions that will be in that window:

STATIC IP Each connection can be set to a static IP. This allows for manually assigning the WiFiRanger with a static IP by Device. This feature is useful if connecting to an internet source that does not issue DHCP addresses. In these cases, assign a Static IP Address within the source's IP scheme and enter the corresponding Subnet Mask and Gateway IP. Once a Static IP is configured for the appropriate Device, connect to the non-DHCP internet source.

SPEED TEST Controls whether or not a speed test will automatically be performed when this source is connected to.

MINIMUM ACCEPTABLE SPEED Defines a download speed below which this connection shouldn't be used. Speedtests will be run at intervals determined by the "Minimum Speed" Test dropdown on the Setup pagel. If the speed of a connection is less than its defined "minimum acceptable speed" it will no longer be considered to be active. This feature is independent of MultiWAN setting or on whether or not Usage Tracking has been enabled. Using this feature requires that both Fallover and Speed Test (for that connection) be enabled. To set the minimum speed, move the slider to the speed you want and save.

INTERNAL WIFI All Rangers have at least one internal WiFi radio which can be used to connect to WiFi access points. Some Rangers have a single 2.4 GHz radio; some have both 2.4 and 5.8 GHz radios. To use a Ranger's internal radio it is necessary to have a check in the Enabled column of the Setup page in the line for that radio. If your Ranger has both 2.4 and 5.9 GHz radios and you want to use both, you will need to place checks in the Enabled column on both lines.

It is important to note that the Internal WiFi line(s) on the Setup page have nothing to do with the WiFi broadcast(s) that your Ranger creates for your networked device to connect to.

You could, for example, not activate the Ranger's internal radio and yet still have the Ranger broadcast a WiFi signal for your devices to connect to. Think of the Setup page connections as being to the "outside world" whereas the Ranger's WiFi broadcast is for the use of your devices (your local world).

WFRCONTROL If you have a dual Ranger system, there will be a check in the Enabled column for WFR Control. As you verified in the Quick Start guide, clicking on the Settings gear on the right side of the WFRControl line will open a window in which you can verify that WFR control is in use. Ordinarily, you will not have occasion to make changes to settings that can be accessed through this line.

ETHERNET WAN All indoor Ranger routers have Ethernet ports which can be configured as WAN ports to be used for connecting to some cellular hotspots, cable or fiber modems, DSL modems, etc. To use an Ethernet port as a WAN port is is necessary to put a check in the Enabled column on the Ethernet (or Ethernet 2) WAN line and save that change. In addition it is also necessary to click on the Settings gear on the right side of that same line. A window will open in which you can specifiy which of the Ranger's LAN ports will be used as a WAN port in your system. Even though one of the ports may be physically labeled as being for WAN, the designation on the Setting page will override that.

It is important to note that the WAN port is for connecting to an "external" internet connection; the remaining LAN ports are for connecting devices, such as laptops, if they have Ethernet ports.

A second Ethernet WAN port can be assigned if you desire to have two Ethernet WAN internet sources. Simply check Ethernet WAN 2 as Active, then expand its Settings to select which port to assign for the secondary Ethernet WAN.

CELLULAR The primary use of the cellular line on the Setup page is to activate and control the operation of embedded cellular modems that can be found in many WiFiRanger routers. Rooftop Ranger models Denali, Teton, Sky4 and SkyPro LTE can each support one modem and their Setup pages will show a single cellular line. Placing a check in the Enabled column of those lines, will enable and disable the modem.

However, indoor WiFiRanger routers (Poplar, Spruce, Aspen, Core and GoAC) will display multiple cellular lines on their Setup pages; the lines are labeled Cellular 1, Cellular 2 and Cellular 3. Those additional cellular lines are for USB-connected hotspots and/or smart phones which can be "tethered" to the Ranger using the router's USB port. A detailed discussion of tethering is found in Section 3.

WFRBOOST CPE This option is provided for advanced users who wish to connect their Rangers to "customer provided equipment". It is not recommended for use by most customers

Note: Regardless which specific internet connections you choose to enable, it is strongly suggested that you list them on the setup tab in the preferred order of their use. The list can easily be reordered by using the up/down arrows on the left side of each line or by manually changing the number at the left of each line. Any changes made should be saved using the button at the bottom of the tab.

2d USING THE CONTROL PANEL'S MAIN PAGE TO SCAN FOR AND SELECT NETWORKS

The Main page of the control panel was introduced in the Quick Start section of this guide; in this section its use will be discussed in more detail. The Main page provides a lot more data than just a list of available WiFi networks. It contains lots of information which can help you select which network you wish to connect to. The WiFi broadcasts are displayed in decreasing order of their measured signal strength. The names shown in the list are those given to that broadcast by its "owner". You may often hear people refer to those broadcast names as the "SSID" of that access point where SSID stands for Signal Set Identifier.

The Signal column of the display provides a simple graphic depiction of the signal strength and "mousing over" this graphic will display a pop-up which shows the signal strength in decibels as shown in Figure 2d-1 In general, stronger signals are preferable to weaker ones, but don't forget that signal strength is expressed in negative decibels, so a smaller number represents a stronger signal.

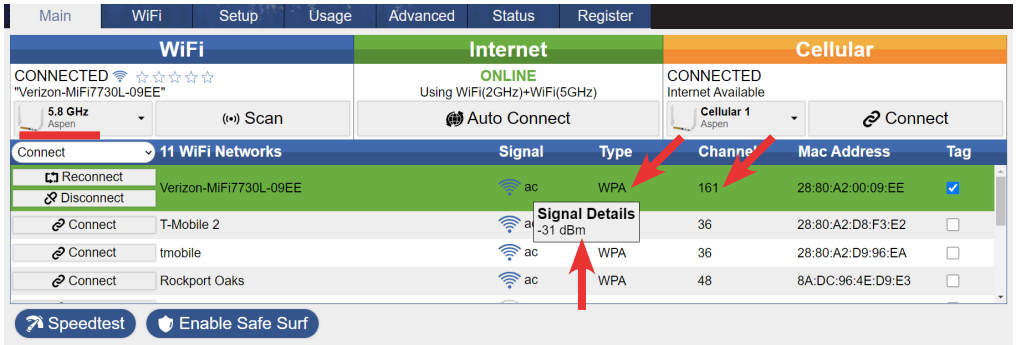

FIGURE 2d-1

To the immediate right of the signal strength graphic are letters which provide information as to the WiFi specification which that access point is using. In the previous figure all the signals are labeled "ac" because it was obtained using the Aspen's 5.8GHz radio and most access points broadcasting in that band will operate in accordance with IEEE standard 802.11ac.

The column labeled "Type" tells us the type of encryption security the access point is using. If the word OPEN appears instead of an encryption type, that indicates that no encryption is being used and that access point will not have a password associated with it. The Ranger will automatically detect and connect to all common types of encrypted networks.

The next column to the right is labeled Channel and it displays the channel that the access point on that line is using. 2.4 GHz WiFi uses channels 1-11 and 5.8 GHz WiFi uses channels 36-165. It should be noted that the access point determines the channel, not the Ranger or other device being connected. Settings on the WiFi tab of the control panel will not affect the channel that is used for a particular connection.

The 5.8 GHz band has far more available channels than does the 2.4 GHz band which means that there is less chance that different WiFi sources will interfere with each other. Furthermore, the broadcast standard for the 5.8 GHz band provides for significantly more signal bandwidth than is available at 2.4 GHz. So, in general, if you are connecting to an access point that has both 2.4 and 5.8 GHz signals, you will get better performance from the 5.8 GHz one. However, 5.8 GHz signals don't travel as well over long distances and are more readily attenuated by building walls, trees and other obstacles. That's why it's important to check the signal strength of the signals you are considering connecting to.

2e SELECTING A NETWORK TO CONNECT TO

Quite often choosing a network to connect to is simple. For example, if you are connecting to your cellular hotspot it may have only a single SSID available. If it has both 2.4 GHz and 5.8 GHz SSIDs then the better choice will usually be the 5.8 GHz signal assuming that the signal strengths are comparable.

At RV parks and other similar locations, you may find that the Ranger displays several identical SSIDs at either 2.4 or 5.8 GHz, or both. This can happen if the park has several different access point sites throughout the park. Most likely your laptop or phone will show only a single SSID while your Ranger may display several with the same name. If you look closely, you will see that the column labeled MAC address shows a different value for each WiFi even though the SSIDs are the same. That's because the Ranger is "seeing" each access point separately. Depending on how the network is constructed, that may permit you to connect to a specific access point which may be faster or less congested than the one that might have the strongest signal. However, it's also possible that the network won't permit you to connect to the SSID of your choice and it will assign one regardless of which one you attempt to connect to. We'll discuss more about this in the "Ranging" section of the Advanced Topics chapter of this guide

When you decide on a network to connect to, simply click on the CONNECT button on the left side of the line you have selected. In the WiFi box at the top of the SSID list you will be able to observe the steps involved in connecting to the selected broadcast. If a Network Key (password) is required, you will be prompted to enter it. As with any computer password, be careful to enter it exactly as it has been provided to you. (If the SSID is listed as OPEN in the "Type" column, a password won't be requested, but the network may still be using a "splash page" as a simple form of security. The next section on Filtered Networks will discuss splash pages in more detail.)

After the connection has been completed the WiFi box should display CONNECTED and the Internet box to the right of it should show ONLINE. As shown in the figure, the selected SSID will now have a green highlight.

Once the SSID line has turned green, the CONNECT button will change to two buttons, RECONNECT and DISCONNECT as shown on the T-Mobile line in the previous figure.
The purpose of the DISCONNECT button is obvious; the RECONNECT button should be used if there appear to be problems with the Ranger's connection to that WiFi broadcast.
In particular, if you were to observe that the highlight on the line had changed from green to yellow, that would be an indication that data isn't flowing through that connection. It could be a problem at the access point or it could be an issue with the Ranger's connection to it.
In either case, the first thing to do would be to click on the RECONNECT button to see you can re-establish a good connection. When you do that the Ranger will reconnect to the same SSID and often that will cause the line to return once again have a green highlight.

2f CONNECTING TO FILTERED NETWORKS (SPLASH SCREENS)

Sometimes the operator of a WiFi network chooses not to use encryption to control access but still wishes to exercise some degree of control over users. This is often found with the "free WiFi" provided by retail stores, hotels, RV parks, etc. In those cases the network manager will create a "splash page" that displays during the connection process. The splash page typically presents terms and conditions for usage of the WiFi and often requires the use to provide some identifying information such as name and site or room number.
Until the splash screen conditions have been complied with, data will not flow through the internet connection.

Splash screens have traditionally been difficult for routers to deal with but version 7.1.0b11 (and later) of the WiFiRanger firmware "negotiates" with a WiFi access point so that the splash page is automatically presented to the user. Upon entry of the appropriate information onto the splash page, the user is then free to use the internet connection.
The process can take ~30 seconds to complete, depending on the nature of the WiFi system you are connecting to.

If the automatic process does not, itself, present the splash page to the user, the Ranger will indicate the presence of such a page by presenting the text "Filtered Network—Click to Connect" in the top center box of the control panel Main page. Clicking on that text will then take the user to the splash page.

(It should be noted that for the Filtered Networks process to function successfully, the Control Panel Redirect switch in the middle of the Setup page must be set to ON.)

2g CUSTOMIZING YOUR RANGER'S WIFI SETTINGS

All WiFiRanger routers are capable of supporting both a private network and a guest WiFi network. Settings for these networks are controlled on the WiFi tab of the Ranger's control panel. By default, the guest network is disabled, and the private network is what is used in most cases. In some RV installations the guest network is used for data exchange between subsystems of the RV; in those cases no changes should be made to the guest network settings.

The WiFi tab is where you can change the password and WiFi broadcast name (SSID) of your Ranger. Figure 2g-1 is a screenshot that shows the section of the WiFi tab that controls those functions. This screenshot was taken from an Aspen router that has both 2.4 GHz and 5 GHz broadcasts, so the figure shows SSIDs and passwords for both. Your Ranger may have only a 2.4 GHz broadcast so you may see only one set of controls.

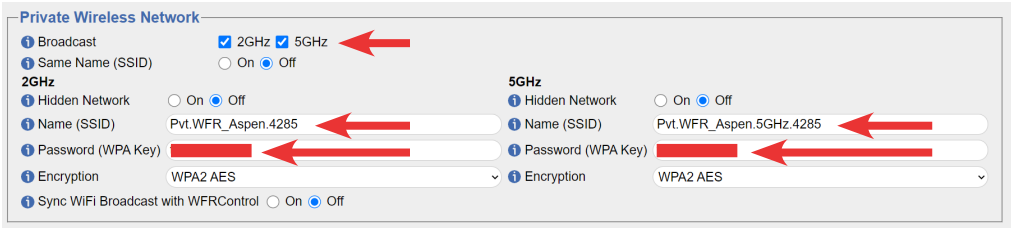

FIGURE 2g-1

You can rename your SSIDs and passwords as you wish but you are encouraged to use alphanumeric characters only. Some “special” characters may cause problems for devices attempting to connect. Enter your SSIDs and passwords and save by clicking on the button at the bottom of the page. Please note that changing these could result in the device you are connecting with being disconnected from the Ranger. If that occurs just reconnect to the renamed SSID using your new password.

The remainder of the WiFi tab contains less-frequently used controls which will be discussed in the later, advanced sections of this guide.

2h UPDATING THE RANGER’S FIRMWARE (EMBEDDED SOFTWARE)

It is very important to keep your Ranger’s firmware updated so that it always has the latest available version. Doing so ensures that your device will operate as effectively as possible

In the upper right-hand corner of every page of the control panel is a link that normally reads Check for Updates. Clicking on that link until blue bars start to scroll forces a manual check for updates, but automatic checks for updates are made periodically whenever the Ranger is connected to the internet. When an available update is found, the link will and will read Update Firmware. Clicking on that link will begin the 10-15 minute update process. It is important that the Ranger be connected to a reliable internet source during an update, a cellular hotspot or your home WiFi would be excellent choices.

The update process is fully automatic. When it has completed, the Ranger will reboot using the new firmware. In the upper right corner of any control panel page the firmware version is displayed, and you will be able to verify that it has changed, reflecting the update.

Although often overlooked, registering your WiFiRanger is important to keeping it updated with the latest firmware (embedded software). Your Ranger cannot be updated unless you fill in the information on the Register tab of the control panel. At a minimum you must supply your name and email address. If you do not register you will not be permitted to download updates.

3 CONNECTING TO CELLULAR NETWORKS

3a USING EMBEDDED CELLULAR MODEMS

Embedded cellular modems can be located in either rooftop or indoor Ranger routers. The basic process for getting online with a modem is the same regardless of location. In either case the user must first decide which cellular carrier and which specific data plan is right for them. WiFiRanger routers all can be used with AT&T FreedomGo plans sold by Winegard but they are not locked to those plans; most AT&T and T-Mobile data-only plans (the kind used for hotspots) will work with embedded modems in WiFiRanger routers.

Once a data plan has been decided upon, the first step is to insert the SIM into the modem. Although this is simple, it is important to orient the SIM properly in the "slot". All WiFiRanger routers use "full-size" SIMs which are rectangular with one diagonally cut corner. SIM slots have diagrams associated with them which depict the correct orientation of the SIM when it is inserted in the slot. The diagrams show the orientation of the "cut corner". If your SIM is oriented as shown in the diagram it will make proper electrical contact. There is no requirement to power down the router when inserting or removing a SIM, but it is a recommended practice to do so.

Once the SIM has been inserted, the next step is to activate the modem in the Ranger. Regardless of whether the modem is in an indoor Ranger or in a rooftop one, the Setup page of the control panel will show which Cellular line is associated with it. Usually, the modem will display as the Cellular 1 connection, but that isn't guaranteed.

Figure 3a-1 shows the Setup page of an Aspen router with a modem that is displaying as Cellular 2. A check has been placed in the Enabled column which is the key activating step. The IMEI is shown; the SIM box is blank because a SIM has not yet been inserted.

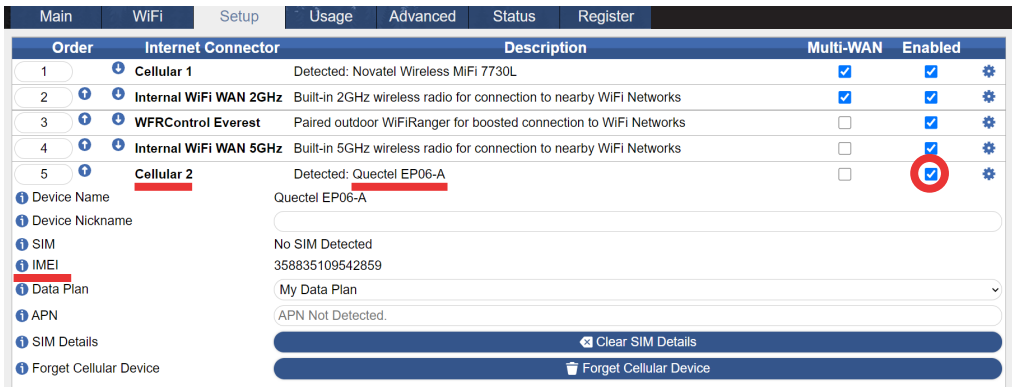

FIGURE 3a-1

Figure 3a-2 shows the dropdown which enables users to choose between FreedomGo and other data plans. The dropdown defaults to My Data Plan as shown in the previous figure.

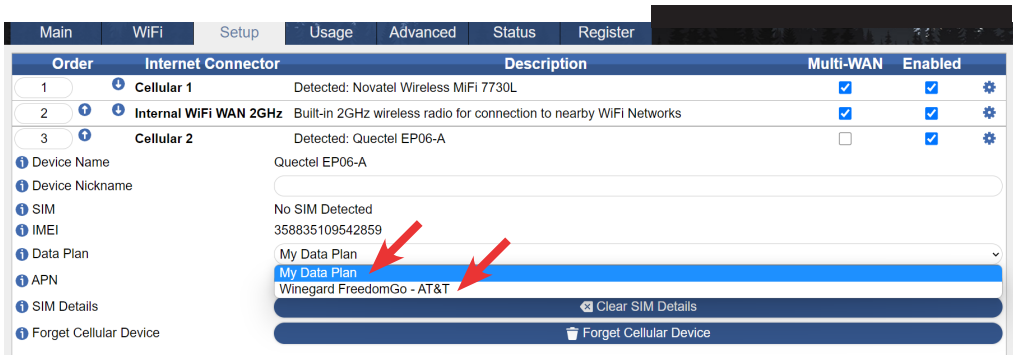

FIGURE 3a-2

Users who choose to use FreedomGo plans do not have to enter any further information. When the FreedomGo dropdown is selected in the previous figure, a link appears for purchasing data plans. That link takes the user to the Winegard site where the purchase can be made. No further action is required. If you purchase a FreedomGo data plan it will automatically become active in 12-36 hours.

Users who choose to use other cellular plans will need to enter the APN (Access Point Name) for the network they have chosen. Entering the appropriate APN will prepare the system for connecting via cellular. The APNs for the three major cellular carriers are:

- Verizon vzwinternet
- AT&T broadband
- T-Mobile fast.t-mobile.com

After entering the APN be sure to save the action by using the button at the bottom of the page. In order to obtain a cellular plan appropriate for your Ranger, you will probably be asked to provide the device's IMEI number which is a unique identifier which tells the cellular carrier what specific equipment is being connected to the cellular network.

After inserting your SIM also be sure to check that the SIM number appears in the window.

Note: Although there are other text boxes and dropdowns visible in the Cellular window, under most circumstances the only user entry that need be made will be for the APN. Making other changes or entering data in other boxes may have serious negative effects and may make it impossible to achieve a connection.

Once these steps have been taken (for FreedomGo SIMs and all others), all that is necessary is to click on the Connect button in the Cellular box on the main page of the control panel. You will be able to observe the text that appears in the Cellular box as the Ranger connects to the network.

Do not be confused if the text reads "Data Connection Available—Click for Internet". That is telling you that the modem has made a "background connection" to the network, but data isn't yet flowing. You still need to click the Connect button to complete the connection. When the modem has completed connecting the text should read "Data Connection—Using Cellular Data".

3b MODEMS IN DUAL-RANGER SYSTEMS— POSSIBLE CONFIGURATIONS

In the previous section only single-Ranger systems were considered. Dual Ranger systems introduce a bit more complexity, but the basic operational functions are still the same. With a dual Ranger system, there are three different configurations to consider:

1 **Modem embedded in indoor Ranger/rooftop Ranger has no modem**
In this configuration the rooftop Ranger (for example, a Sky4 or an EliteAC) doesn't play a role in connecting to the cellular network. As a result, it can be ignored in the connection process and the instructions provided in Section 3a apply with no change and no further discussion is necessary.

2 **Modem embedded in rooftop Ranger/indoor Ranger has no modem**
In this configuration the modem is in a rooftop Ranger which is operated using WFRControl by the indoor Ranger. This configuration will be discussed in detail in the next section.

3 **Modems are embedded in both rooftop Ranger and indoor Ranger**
This case is a composite of the two other cases, and it can be treated using the techniques described for those cases.

3c MANAGING A DUAL RANGER SYSTEM WITH EMBEDDED MODEM IN ROOFTOP ROUTER

To access the modem in the rooftop Ranger you need to go to the **Setup page of the indoor Ranger's control panel**. On the Setup page, find the line labeled WFRControl and click on the gear on the right side of line. A window will open. Figure 3c-1 shows an example of what will be in that window. The window displays a miniature version of the control panel of the rooftop router. In this screenshot the rooftop router is an Everest, but the basic contents of the window will remain roughly the same regardless of which rooftop Ranger you have.

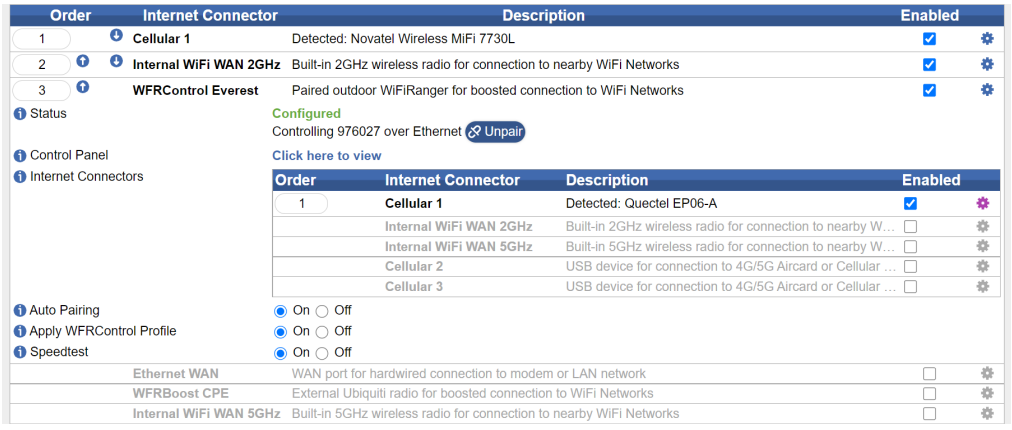

FIGURE 3c-1

This window allows you to control the modem in the rooftop Ranger as if you were directly dealing with that Ranger's control panel. You activate the Cellular connection in the rooftop router by putting a check into the Enabled column of the Cellular 1 line inside the window and save by clicking on the button at the bottom of the page.

One important thing to note when working with this configuration is that the Cellular line on the Setup page of your **indoor** Ranger's control panel has **nothing** to do with the operation of the modem in the rooftop Ranger. There is no reason to activate any of the Cellular lines on the indoor Ranger unless you plan on tethering a hotspot or phone to the device. If you don't plan on tethering, leave the Cellular lines disabled.

Another important point to note is that since the rooftop Ranger is being controlled under WFRControl, it can only perform one task at a time. For example, if you have a Denali with a modem and its WiFi radio, it can only bring its data into the indoor Ranger to which it is connected using one of these connections of the other. To say it another way, if you want to use the modem in the Denali, you can't, at the same time, use the Denali's internal WiFi radio.

This also means that if you have an Everest with two modems and a WiFi radio, **you can only use one of these at a time** when the Everest is being operated under WFRControl.

At present, the only way around this limitation is to unpair the indoor and rooftop Rangers which allows you to operate a MultiWAN with the capabilities of the outdoor Ranger. This is discussed in detail in Section 5.

3d TETHERING OF CELLULAR DEVICES

Indoor WiFiRanger routers (Poplar, Spruce, Aspen, Core and GoAC) will display multiple cellular lines on their Setup pages; the lines are labeled Cellular 1, Cellular 2 and Cellular 3. Those additional cellular lines are for USB-connected hotspots and/or smart phones which can be "tethered" to the Ranger using the router's USB port. A tethered cellular device will, in many respects, operate similarly to an embedded cellular modem.

To tether a device to a Ranger it is first necessary to place a check in the Enabled column for the appropriate line. If more than one device is to be tethered at one time, a powered USB hub will also be required. Once the appropriate cellular line has been enabled, additional drop-down CONNECT buttons will be created in the Cellular area on the upper right portion of the control panel Main page.

Figure 3d-1 is a screenshot of the Setup page for an Aspen router which has a tethered Novatel 7730L hotspot displaying as Cellular 1 and an embedded Quectel modem displaying as Cellular 2.

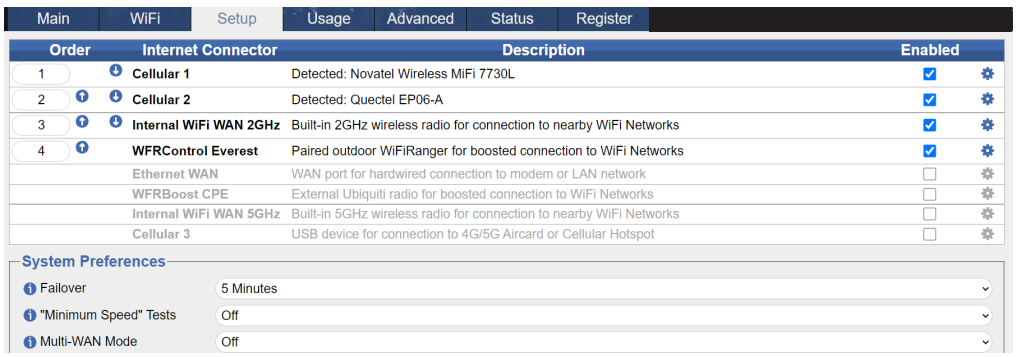

FIGURE 3d-1

Figure 3d-2 shows how those multiple cellular connections result in multiple cellular drop-down choices in the Cellular box of this same Aspen.

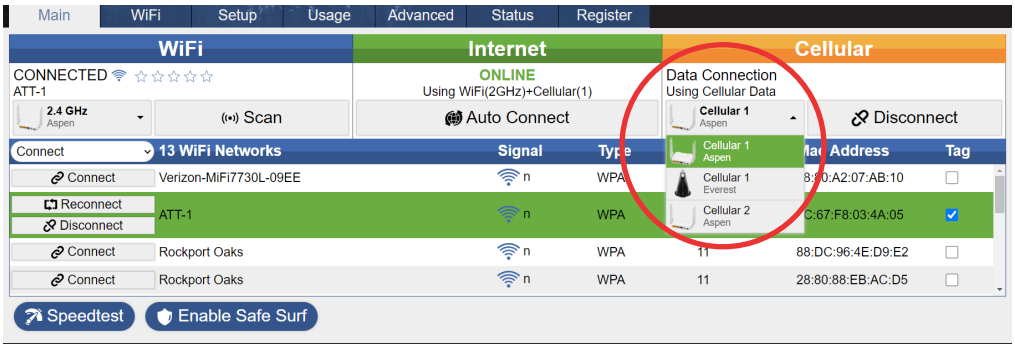

FIGURE 3d-2

It should be noted that to tether a hotspot or phone to an indoor Ranger, it will be necessary to set up that device so that the USB tether is used for both power and data. The settings for that will be in that device's admin control software. Both Android and iOS devices can be tethered, the specific setup requirements will vary from device to device.

When the hotspot or phone has successfully been connected to the Ranger, the text in the Cellular box will read "**Data Connection—Using Cellular Data**" as shown in the previous figure.

4 ADVANCED WIFIRANGER FEATURES

4a ADVANCED USE OF THE CONTROL PANEL MAIN TAB

i. Main Tab Overview Although the Control Panel's Main has previously been discussed, in this section of the Guide, we will examine its display and function in more detail. Figure 4a-1 is the Main tab for an Aspen router. Your Main tab will have some differences, but, overall, it will look very similar.

Notice the text box in the upper right corner of the page; this box appears on every screen of the control panel. It contains five elements:

1. Check for Updates Link—The presence of the blue "check for updates link" indicates that your Ranger has made a cloud-based connection to the WiFiRanger server. If the text Cloud Disconnected were to appear, clicking on the text a couple of times until blue bars start scrolling will restore the link. If the text reads Update Firmware you can initiate an update using the procedures discussed in section 2h of this guide.

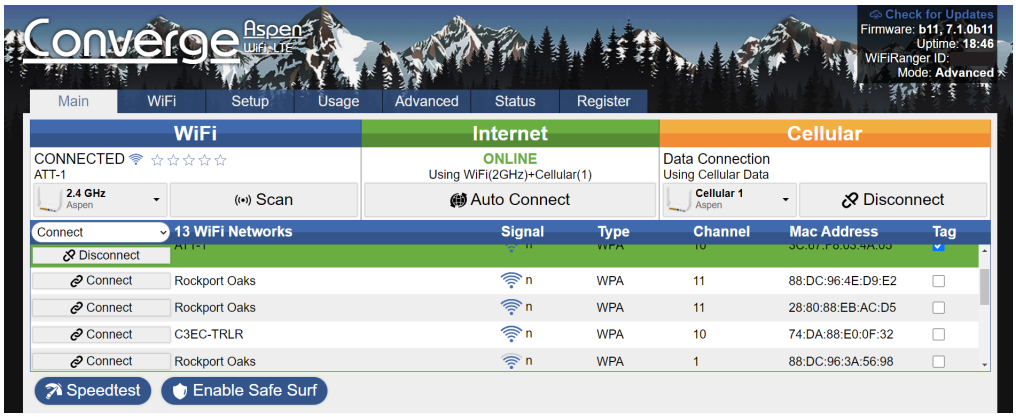

FIGURE 4a-1

2. Firmware Version—Displays the firmware version being used by your Ranger.

3. Uptime—Displays the length of time the Ranger has been operating since it was last booted.

4. WiFiRanger ID—The complete 6-digit ID of the Ranger; each Ranger router has a unique ID which is essential if you were to request trouble-shooting assistance.

5. Mode (Simple or Advanced)—Ranger routers are, by default set to Simple mode in which some more advanced features are hidden from view. This guide has been written with the assumption that the mode has been set to Advanced. Setting the mode is discussed in Section 4ci-i.

ii. **SafeSurf™** Safesurf is a VPN (virtual private network) that is built into WiFiRanger firmware. Safesurf is available for use regardless of whether you are using WiFi, cellular or any other internet connection method. SafeSurf is enabled by clicking on the Enable SafeSurf button at the bottom of the control panel main tab. The VPN that is formed by enabling SafeSurf has your Ranger as one of its endpoints with the other being the WiFiRanger servers in Idaho.

For the purpose of this user guide, it is assumed that the reader understands the general purpose of using a VPN and has some general idea how VPN's work.
For a simple explanation of what a VPN is more information can be obtained here:
https://wifiranger.com/how-is-a-vpn-like-a-phone-booth/

When SafeSurf is enabled a lock symbol appears next to the "Online" text in the center top box on the control panel main page. There can be a brief delay in the appearance of this symbol from when the "Enable SafeSurf" button is clicked on. **The VPN is not functional until the symbol appears.** Also, due to the nature of VPNs, there is always a possibility that SafeSurf might become disabled while it is in use. If that happens the lock symbol will disappear.

Figure 4a-2 shows the SafeSurf lock symbol on the control panel Main tab.

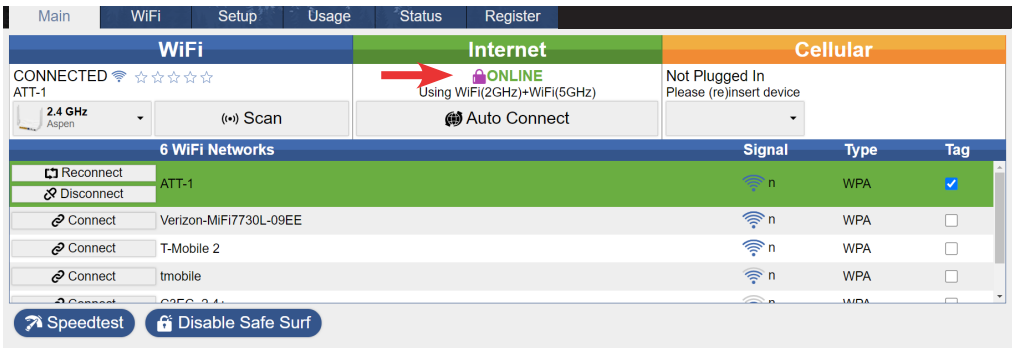

FIGURE 4a-2

iii. **Tagging Networks**—When the number of available WiFi networks is large or there are specific networks that you prefer the Ranger connect or not connect to, the tagging feature can be helpful. Place a check in the "Tag" column on the Main page of the Control Panel for any of the displayed SSISs the Ranger will then prompt you to define the type of tag you wish to apply.

As shown in Figure 4a-3 networks can be designated as Preferred, Ignored, or Last Try. The Ignore function can be particularly helpful when there are multiple "open" networks available, and you prefer that the Ranger not connect to them.

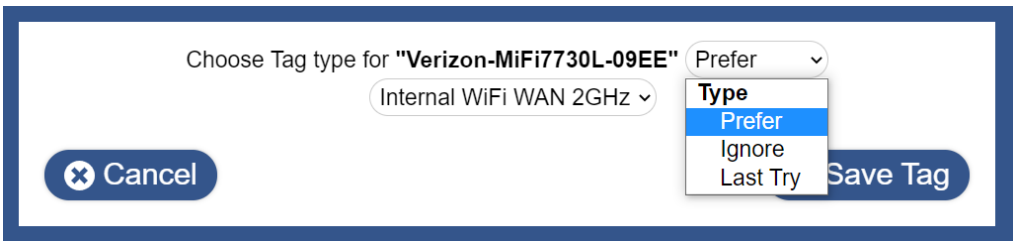

FIGURE 4a-3

The Tagging dialog box can also specify if the tag is to be applied to all internet connections or just the one that you are using at the time the tag is applied. This can be helpful if you prefer that specific SSIDs connect using a specific connection method. This is shown in Figure 4a-4.

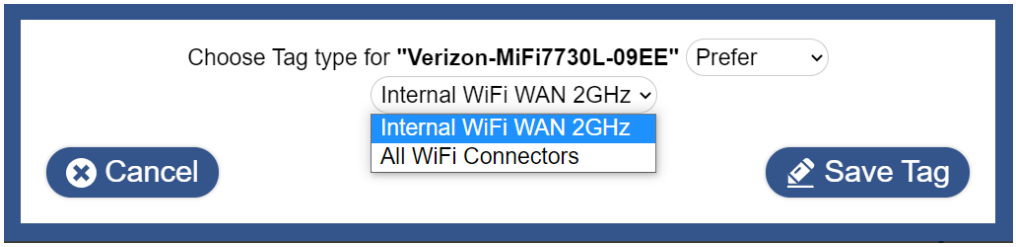

FIGURE 4a-4

Lastly, if there are SSIDs with similar multi-part names then you will be prompted to specify if you want the tag to apply to the entire name or a single portion of this. For example, if the SSID was “Jones RV park” you would be prompted to specify if the tag was to apply to “Jones”, “RV”, “park” or “Jones RV Park”

iv. Speed Testing The Ranger has a built-in ability to perform a speed test of any internet connection it is using. This can be helpful if there are several internet connections available for use and you’re trying to determine which one to use. Only connections that you are actually connected to can be tested. If you are using a MultiWAN and have more than one connection in use all of them can be tested at the same time.

For any particular connection, the master control of whether a speed test will be run is determined by a selection made on the Setup page of the control panel. For any connection that has been enabled, click on the gear on the right side of the line; in the window that opens one of the switches determines whether the speed test function for that connection has been enabled.

Figure 4a-5 shows the speed test switch (the arrow shows the gear that has been clicked on to open the window). It should be noted that speed tests can consume non-trivial amounts of data to perform. Therefore, on connections with limited data allowances, speed tests should be performed only when necessary.

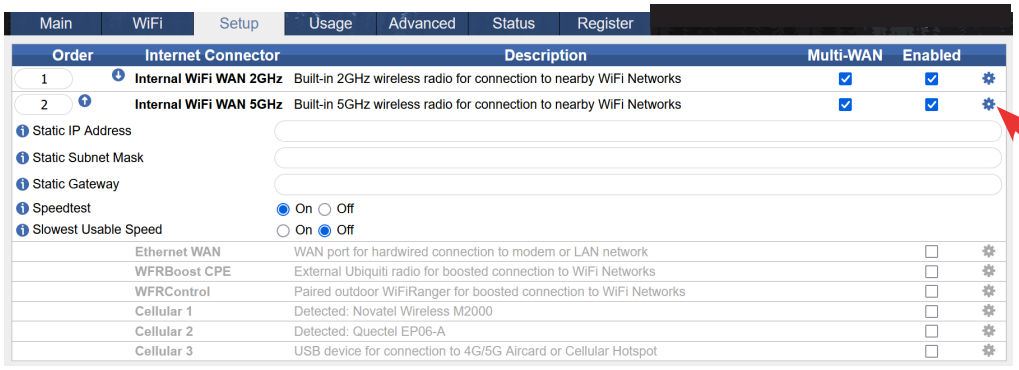

FIGURE 4a-5

Performing a speed test is controlled by the Speed Test button on the bottom of the Main tab. Clicking on the button brings up the window shown in Figure 4a-6.

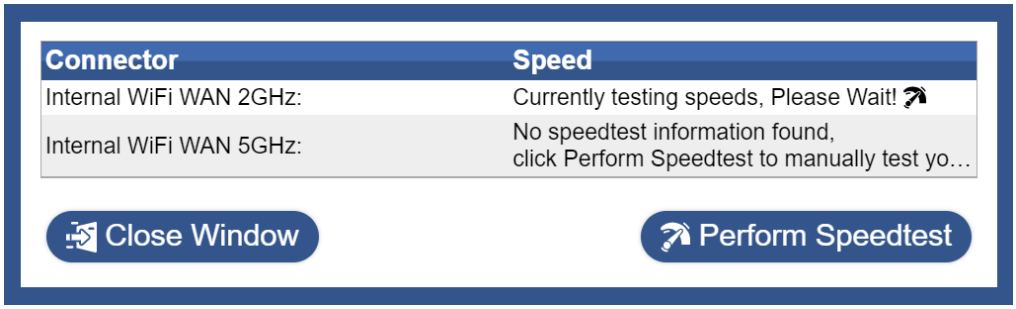

FIGURE 4a-6

In this example, there are two internet connections being used in a MultiWAN setup. Clicking on the Perform Speed Test button will cause the test to begin with one of the active connections. The test can take up to several minutes, depending on the connection. The window can be closed during the test or it can be left open.

Clicking on the Speed Test button on the Main tab again will reopen the window and will display the latest speed test data. If the button is pressed too soon, before the test has been completed, that internet connection will be omitted from the display. Wait a moment for the test to complete and try again

v. **Signal Strength** On the Main tab's list of SSIDs WiFi connections are listed in decreasing order of signal strength. In the signal column a graphic depiction of the relative signal strength of each connection is provided. If you "mouse over" the graphic display, the actual signal strength in decibels will appear as shown in Figure 4a-7. Knowing the precise signal strength can be very helpful if one is attempting to connect to a distant WiFi access point. Repositioning your receiving antenna could increase a marginal signal to the point where it becomes usable.

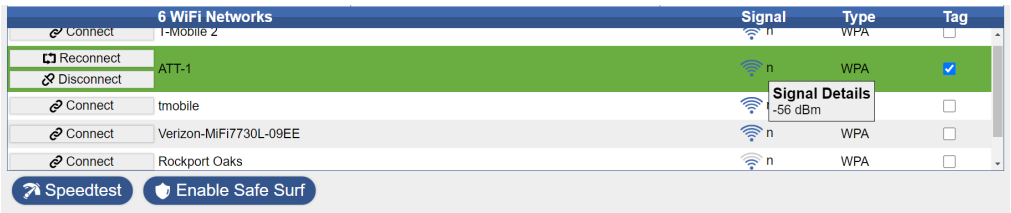

FIGURE 4a-7

vi. Ranging As one moves from one location to another, there will be situations where there exist multiple SSIDs that could be connected to but where the choice of which will provide the best connection can't be predicted in advance. This commonly occurs at RV parks and similar locations where there are multiple WiFi access points to connect to. Although it may seem logical to connect to the one with the strongest signal, that doesn't always guarantee that it will provide the fastest internet connection. That's where the Ranging function can provide helpful data. In Figure 4a-8, a situation is shown where our RV park Rockport Oaks has two access points in range. Although one has a somewhat stronger signal, we'd like to know which one provides the fastest connection and we'd like to be able to know that every time we connect.

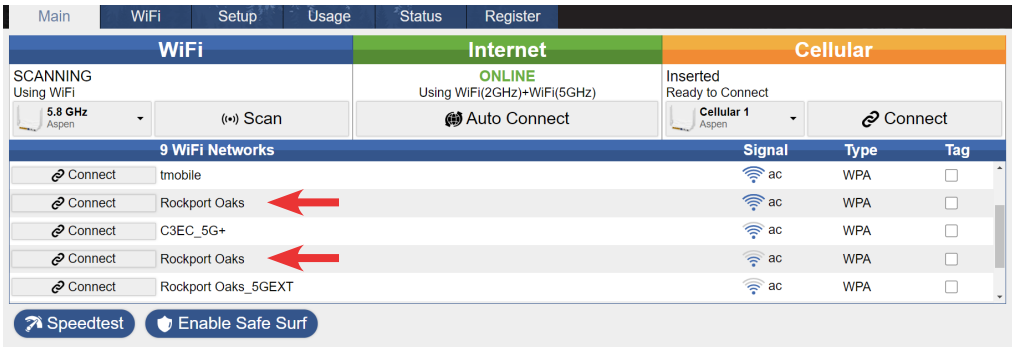

FIGURE 4a-8

The Ranging menu, which is a dropdown under the topmost connect button, provides a way to get that information. Figure 4a-9 displays the Ranging menu available in that dropdown. For our example, the figure also shows that we have tagged the two Rockport Oaks SSIDs so now we can select, from the drop down, the option for "fastest tagged" and the Ranger will automatically test the speeds of both tagged connections and will connect us to the fastest one.

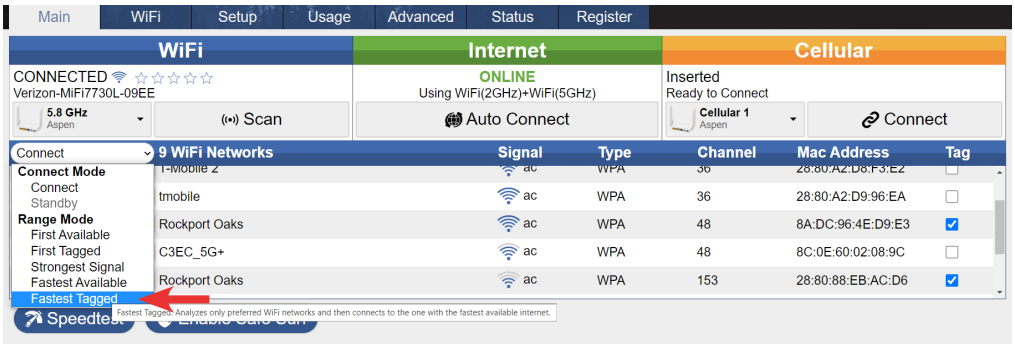

FIGURE 4a-9

vii. Auto Connect The Auto Connect button on the Main tab manually initiates the Failover feature. For a full discussion of Failover, see section 4ci-a.

4b EXPLORING THE CONTROL PANEL WIFI TAB

i. **Stored Network Keys** The top section of the WiFi tab lists all stored network keys (passwords) for networks the Ranger has been connected to. The SSID, password and encryption type are provided for each network. Passwords for stored networks cannot be changed; if a network password has been changed delete the entire line using the delete icon on the right side of the line. When you re-connect to that network you will be prompted to enter the new password.

ii. **WiFi Tags** The second section of the WiFi tab lists all tags that have been applied to WiFi networks. The SSID, type of tag and the connection it applies to are provided. Tags cannot be edited but can be deleted.

iii. **Hidden WiFi Networks** If you connect to networks which are operating as "hidden", their SSIDs can be entered in the third section of the WiFi tab so that they can be connected to with the Ranger.

iv. **Range Options** If you use the Ranging options described in Section 4a-6 of this guide, the range options provided in the fourth section of the WiFi page allow you to tailor the ranging function so that specific restrictions are placed on all ranging attempts. This can be helpful if you wanted to, for example, restrict all ranging to just tagged connections.

v. **Private WiFi Networks** This section of the WiFi tab was discussed previously in Section 3g of this guide. However, several advanced features were omitted from that discussion.

Same name (SSID)—WiFiRanger routers with dual band (2.4 GHz and 5.8 GHz) can be operated so that the same SSID is displayed for both bands. This allows connected devices to "roam" between bands, connecting to the best available connection.

Sync broadcast with WFR control—this allows for the use of a single SSID and password for the device operating under WFRControl and the router which is controlling it for the same purpose as noted above.

Hidden network (on/off)—Advanced users may choose to hide their network name (SSID) so it isn't visible to others searching for WiFi signals. For Rangers with dual band capability this can be done for either 2.4 GHz and/or 5 GHz signals. However, users are cautioned that hiding a network can crate serious problems unless they are familiar with how to connect to networks that have been hidden.

Private Network —The 2.4 GHz and/or 5 GHz private wireless networks can be disabled by removing the checks from the corresponding boxes. This might be something a user wanted to do if he planned to connect to an indoor Ranger entirely by Ethernet. However, turning off the WiFi network for a rooftop Ranger that doesn't have an indoor "companion" can result in a device that cannot be connected to at all. In such cases, it may be necessary to perform a factory reset to be able to regain communication with that Ranger. Care should be taken before a decision is made to disable all WiFi broadcasts.

OEM Management Networks—If your WiFiRanger was installed in a motorhome during manufacture, it is possible that there exists a hidden management WiFi network which is utilized by hardware in the coach to pass information between different subsystems. It is recommended that you not make any changes to this network without first consulting with the manufacturer of your coach.

vi. **Guest Wireless Network** Your Ranger has the capability of supporting a completely separate WiFi network that you could use, for example, as a way of sharing your internet connection with other people at a campground. You can create a separate password for the guest network, and you can set the length of time and how often users can connect to it. You can even create a "professional" environment by setting up a "redirect" webpage that users are taken to while logging in. By default the guest network is off.

vii. **Exploit the Capabilities of your WiFi/Social Networking** Your Ranger has the ability to add to its SSID information regarding services you might provide, services you are seeking or other general information about yourself and your interests. When you click on any of the "banners" in this section, such as "Services I offer" you are presented with a list of options from which you can select one or more. In addition, you can provide identifying information, such as your site number, phone number or email address, so others can contact you about your services. This information is then displayed when another WiFiRanger user sees your SSID and "mouses over it".

Figure 4b-1 shows, as an example, the list of services that could be offered in this manner.

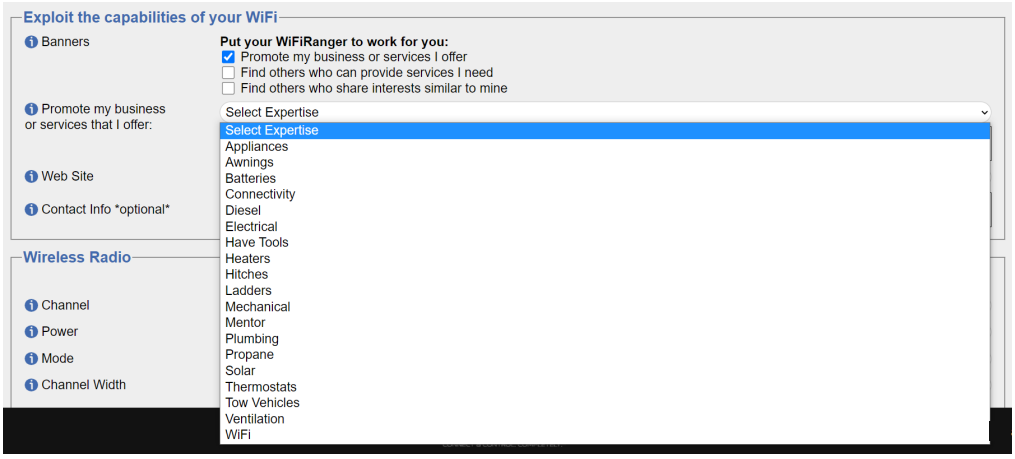

FIGURE 4b-1

If a WiFiRanger owner in your vicinity has activated this feature of his Ranger, you will see a “person” icon displayed next to his WiFi Network (SSID) on the Main tab of the Control Panel. Hover over the person icon to view his interests, skills or needs. You do not need to connect to his WiFi in order to see his info, as a simple WiFi scan will display the icon. Figure 4b-2 shows the Main page of a Ranger where several nearby SSIDs are exhibiting their information and one is being displayed in detail.

FIGURE 4b-2

vii. Wireless Radio This last section of the WiFi tab controls the configuration of the Ranger’s WiFi radios. The default settings for WiFi channel is Automatic for both 2.4 GHz and 5.8 GHz radios but those can be changed if there a reason for doing so. The 2.4 GHz band is often overcrowded at campgrounds and other public locations and, if you notice that, it may be beneficial to change to a less crowded channel. This is less likely to happen on the 5.8 GHz band because of the large number of channels.

The default power setting for both bands is also Automatic. In most cases, the Automatic setting will provide the best results. Indiscriminate use of high power WiFi can create unwanted interference, both for you and others.

Most users will be best served by leaving the Mode switch in its default channel width setting of 20 MHz which should be satisfactory for most purposes. 5 GHz broadcasts can utilize bandwidths as large as 80MHz and advanced users may choose to change the setting to Automatic which will permit use of increased bandwidth.

4c ADVANCED SETUP TAB CONTROLS

i. **System Preferences** The Setup tab contains several important configuration settings

a. Failover—Automatically attempts to connect the Ranger to the activated connections in the order in which they are listed on the Setup tab. This is why the proper ordering of connections is important. WiFiRangers are shipped with Failover disabled to avoid creating a re-connect loop if no initial internet connection is available when the device is first connected. However, once the user has become familiar with the Ranger, most users will find it helpful to have Failover enabled all the time. When Failover is enabled, the reconnection attempt will occur after the selected interval has expired. The AutoConnect button on the Main tab will manually cause the Failover process to initiate regardless of the interval selected.

b. "Minimum Speed" Tests—This dropdown is the master switch which enables the Minimum Acceptable Speed slider on any internet connection where the user chooses to use it. The interval set by the dropdown specifies how often speed tests will be run for any connections for which it has been enabled. For the Minimum Acceptable Speed feature to be operational, Failover has to be enabled as well as speed testing for the selected connection.

c. MultiWAN mode—MultiWAN is discussed in detail in Section 5. This switch selects the MultiWAN mode.

d. Control Panel Redirect—when the Ranger is not yet connected to the internet, this switch forces the browser to display the Ranger's control panel. For ease of access to the control panel, it is important that this swtich remain "ON".

e. Initial Auto Connect—Enabling this switch causes the Ranger to attempt to connect to the first enabled connection as part of the boot process. For example, if you turn off your Ranger overnight, this switch will enable it to reconnect to your desired connection when it boots up in the morning.

f. Attempt Auto Login—Automatically attempts to bypass login/agreement page at Filtered WiFi Networks. Public networks that require a username and password cannot be bypassed, but Filtered networks that simply have a one-click access button may be automatically bypassed with this feature on..

g. Sync data—Enabling this switch allows the Ranger to provide signal quality data to WiFiRanger servers

h. Hide Advanced Features—Enabling this switch hides several control panel settings that are intended for use by advanced users. Operating the system in Advanced Mode (Hide Advanced Features set to "off") provides the user with a number of additional features which users they may choose to enable. However, if the Ranger were to be subsequently reverted to Simple Mode all changes made while in Advanced Mode would also be undone. Therefore, it is not generally recommended that systems be reverted once they are set to Advanced Mode. However, it should be noted that performing a Factory Reset using the button on the bottom of the Setup tab will always revert the Ranger to Simple Mode.

ii. **Profiles** For those who change their Ranger's configurations often, Profiles provide an easy way to set a number of parameters at the same time. Several profiles are provided as examples; others are easily added. Profiles can include settings such as "which connections are activated", "the order of the active connections", etc.
Use of profiles is entirely optional. Figure 4c-1 shows an example of a profile in which a tethered MiFi hotspot is used as the primary connection with WiFi being available as an optional backup. In this case Failover has been set to "off" to prevent the connection from changing unless the user directs the action take place.

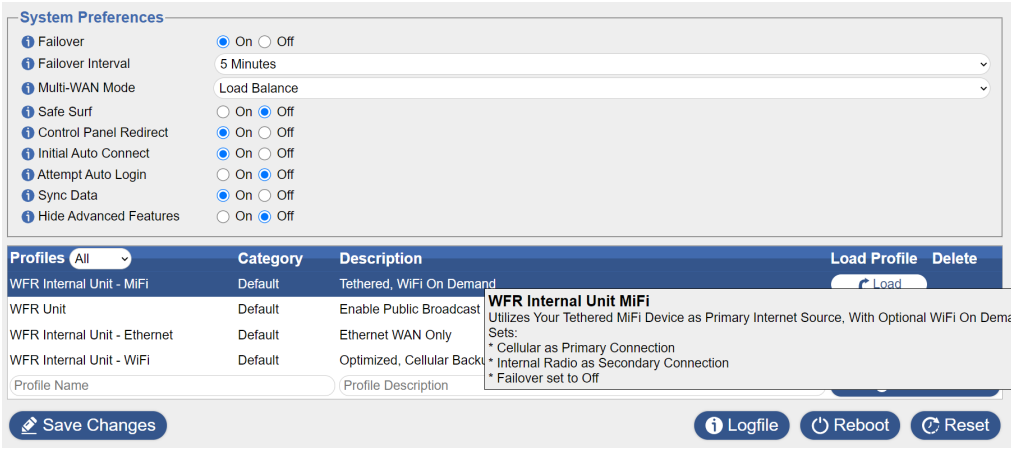

FIGURE 4c-1

Additional profiles can be created and saved. Choose a name for the new profile and create a brief description. Then set the Ranger's configuration settings as you desire them to be and save. When you subsequently load that profile, your settings will be restored

Bottom of the Tab Buttons:

At the bottom of the Setup tab, in addition to the Save button, there are three additional buttons:

Logfile You could be asked by WiFiRanger technical support to download a logfile from your Ranger for diagnostic purposed.
This button will download a logfile.

Reboot This button will initiate a reboot by your Ranger.
Passwords and other stored data will not be reset by this action.

Reset This button will initiate a factory reset of your Ranger.
Stored passwords and other data will be erased.
The Ranger's SSID and password will be returned to their default settings.

4d USAGE TAB

By default the Ranger's usage tab is set to OFF. Enabling usage tracking creates an additional load on the processor and some performance degradation may occur. Unless device restrictions are being implemented, it is probably best to use the Usage tab for diagnostic purposes rather than for extended use. To enable the Ranger's usage tracking features set the Usage switch to "ON" and save.

a. Usage tracking—This is a powerful diagnostic tool for understanding the use of data by the Ranger and the devices connected to it. It is particularly helpful when multiple connections are being used in a MultiWAN configuration.

Figure 4d-1 shows the real-time data utilization graph at the top of the Usage tab. Any active internet connection can be displayed; the selection boxes at the left side of the graph control which of the current connections are being displayed. In the figure, connections using the 2GHz and 5GHz radios are being shown.

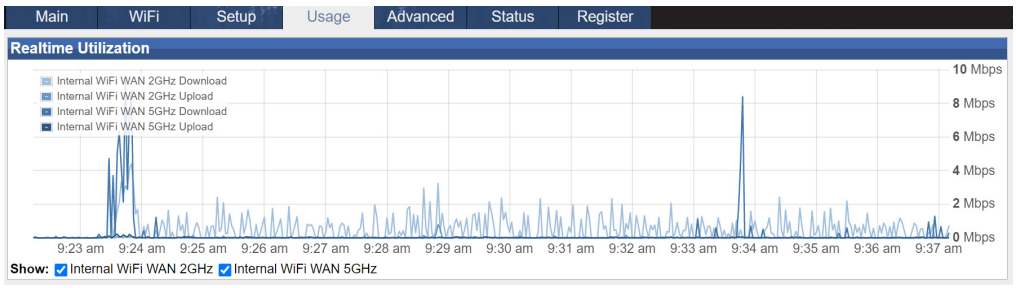

FIGURE 4d-1

A caution about interpreting the data on the real-time graph is that the lines for multiple connections can overlap each other and can create misleading impressions when viewed in the aggregate. For example, in the graph shown, the dark blue line will always display in preference to the light blue line when they overlap. Without examining both graph traces separately it is impossible to know the actual usage of each.

b Bandwidth History—The central portion of the Usage tab displays data used by hour, by device and by internet connection.

Figure 4d-2 is an example of such a history. By clicking on the Show History/Hide History button the display can be togged between data used by each connection per hour and data used by each device on each connection.

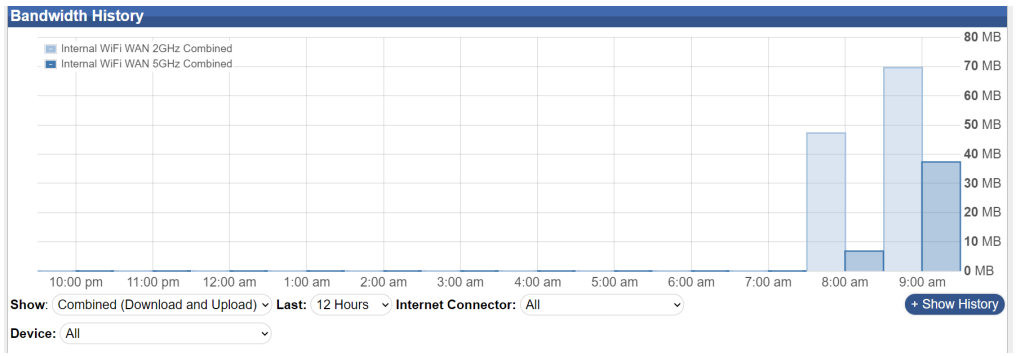

FIGURE 4d-2

c. Bandwidth Groups—This section of the Usage Tab allows for creation of custom groups of internet sources to combine the total data usage into one viewable and trackable statistic. This can help with keeping track of overall usage of a shared 4G plan that may include a MiFi and multiple smart phones. Instead of only having visibility for each individual device on the shared 4G plan, you can lump the sum of their usage together to accurately avoid overages.

Configuring a Bandwidth Group

1. Enter new Group Name under Bandwidth Groups section
2. Select desired color from palate (used for group title and graph bars)
3. Click Add
4. Follow on-screen options to combine desired internet sources into Group
5. Click Add to Group to put another device in the Group
6. Click Save Changes

d. Device Restrictions—Make rules to manage internet speeds or access for specific devices and/or internet connections. This can give you control over bandwidth usage for optimizing performance, limiting usage by particular individuals, and/or avoiding overages on data plans. Device Restrictions could, for example, be used to schedule when children have internet access, to cutoff 4G service when approaching monthly limits, or limiting internet speeds or downloads on particular devices.

Configuring a Device Restriction

1. Select all or a particular Internet Connector or network interface
2. Select all Devices or a particular one
   (check Exclude if effect should apply to all other Devices)
3. Select desired Effect when restriction engages
4. Set Schedule for when restriction applies
5. Set Threshold for amount of bandwidth consumed that triggers the effect
6. Set Reset Interval for timetable that the bandwidth Threshold will be reset on
7. Click Add

A “limit speed” restriction will be highlighted in yellow when active and a “disable internet access” restriction will be highlighted in orange when active. A message will also display on the Control Panel that indicates that the restrictions is in effect. Any restrictions that are not highlighted in yellow or orange are not currently being applied. Figure 4d-3 provides examples of several device restrictions.

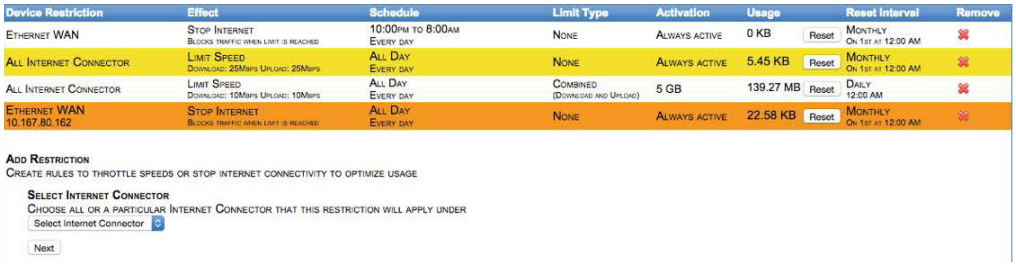

FIGURE 4d-3

4e ADVANCED TAB

The Advanced tab is only visible when Hide Advanced Features on the Setup tab is set to “OFF”. The top section of the Advanced tab allows the user to enable port forwarding for a specified ranger of ports--the user specifies the IP Address of the destination device/ computer, the starting/ending ports, and the protocol in use.

UPnP Services Allows automatic network discovery and function of devices and services

DMZ IP Address On the Advanced tab, set a DMZ IP Address of a server behind the WiFiRanger. DMZ stands for Demilitarized Zone, which in computer security terms means that this server is exposed through the router’s firewall so that access is granted to the DMZ server from the internet. Hosting a DMZ server behind a WiFiRanger does not compromise other devices or computers on the LAN. Only the specified server will be exposed to the internet.

IP Alias Create Private LAN IP Aliases that bridge up to two IP subnets with the WiFiRanger’s unique DHCP subnet. This feature allows for easily placing a WiFiRanger into an existing network that was on a different subnet with statically assigned devices. By creating a Private LAN IP Alias, devices issued a DHCP address will also see anything statically assigned in the IP Alias range. To create an IP alias, enter the desired Gateway IP and Subnet separated by a comma (no spaces).

DNS Usually Domain Name Servers will be automatically obtained through your internet connection(s); however, you can specify a static set of DNS servers. For most purposes the automatic setting should be sufficient. However, occasionally a specific internet connection may fail to provide accurate DNS information. When that happens specifying a set of static DNS servers usually will remedy the issues. The most commonly used static DNS servers are those operated by Google which have the following IP addresses: 8.8.8.8 and 8.8.4.4

Hardware

Router Lights: If you have a reason to disable the LED lights on your Ranger, you can do so with this switch.

USB Power Only: By default, the USB port on an indoor Ranger can be used both to provide power and data tethering. However, if you wish to prohibit use of the port for data, this switch will disable that function.

Admin Access By default, Admin Access is set to “OFF.”
Under some circumstances you may have users of you network who you wish to restrict from having access to the Ranger’s control panel. For example, you might have specified device restrictions to control internet usage by children and you wish to prevent them from undoing those restrictions. In such cases you can enable Admin Access by changing the “Login Required” switch to “ON” and specifying a username and password.
When Admin Access is enabled attempts to access the control panel will be redirected to the Admin Access login screen.

> **Caution:** It should be noted that enabling Admin Access is **not** cleared by a factory Reset; therefore, it you enable Admin Access credentials, be sure not to lose that information. Otherwise, you could lose all access to your Ranger.

4f STATUS TAB

The top section of the Status tab lists the internet connections currently in use by the Ranger and provides specific internal and external address information about them. If you are using only one internet connection at a time, this section will have only a single line.

However, if you operate your Ranger in a MultiWAN configuration as explained in Section :??, the number of lines in the top section of the Status page will correspond to the number of internet connections currently in use. **If the display in the top section of the Status tab were to have yellow highlighting on two or more of the listed connections, this would indicate the presence of an IP address conflict between two or more of your connections which, essentially, would make them unusable until the conflict was corrected.** The topic of how such conflicts come about and how they can be corrected is outside the scope of this guide.

Figure 4f-1 shows the upper section of the Status tab for a Ranger which is operating in a MultiWAN mode with two internet connections. The Default Gateways for the two connections are not the same and, as a result, no IP address conflict exists. Therefore, no yellow highlight is present.

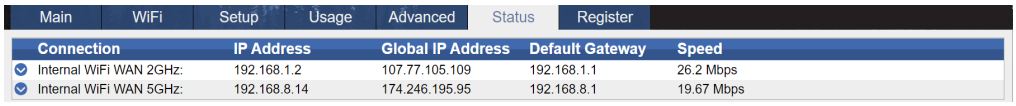

FIGURE 4f-1

However, figure 4f-2 shows the Status tab when two connections have conflicting IP addresses. Notice the yellow highlight on the 5.8GHz and Cellular 1 lines which indicates they are in conflict. When this occurs only one of the conflicting connections will have access to the internet.

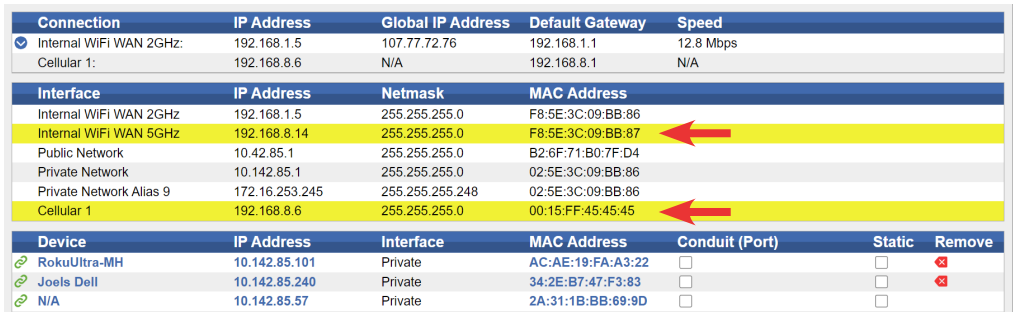

FIGURE 4f-2

The Device section of the Status tab lists all the devices that are currently connected to your private network and those that have recently been connected. The name of each device can be edited by clicking on it and once edited, the device will retain that name for future connections.

The IP and MAC addresses of all devices are shown. The IP address of any device can be converted to “static” by putting a check in the Static box on the appropriate line.

The Device section of the Status tab can also be used to create “conduits” (port forwarding) for devices on your private network by putting a check in the Conduit box and specifying the port to be opened.

Static IP addresses may be required by IP cameras and other smart devices and port forwarding may be needed for gaming and other purposes. Implementing these features is straightforward; explaining how they are used is outside the scope of this guide.

4g REGISTER TAB

Registration of your Ranger by using the Register tab is a requirement for downloading future firmware updates. If you fail to register you will see notification of available updates but will be unable to download them. The minimum amount of information required on the Register page is your name and email address.

Note: At present there is no interconnection between information entered on the Register tab and customer account you may have created at WiFiRanger.com.

5 MULTIWAN OPERATION

Traditionally, a router connects a single internet source to devices on a network. Multiple connections may be available but only a single connection is active at any given time. WiFiRanger's MultiWAN mode enables the user to utilize multiple connections either simultaneously or as backups to each other.

There are two modes for employing MultiWAN. The switch for selecting the MultiWAN mode is found in the System Preferences section of the Setup tab. Until that switch is set the MultiWAN boxes will not appear on the connection lines of the Setup tab.

The specific internet connections to be included in a MultiWAN setup are selected by placing a check in the MultiWAN column of the appropriate line in the upper section of the Setup tab as shown in Figure 5-1. That figure illustrates an Aspen router in which the 2 GHz and radio and Cellular 1 connection are designated as being part of a MultiWAN connection. Also, important to note is that other internet connections are designated as Active but are not involved in the MutliWAN. There is nothing that requires the MultiWAN to use all available connections.

FIGURE 5-1

To decide which available internet connections should be used in a MultiWAN it is necessary to first specify which MultiWAN mode is being used. We will discuss both modes in the following sections.

5a LOAD BALANCE MODE

When Load Balance is selected as the MultiWAN mode, all designated internet connections will share the data flow in what is often referred to as a "round robin" configuration. Data flowing (both downloads and uploads) will shift, in sequence, from one internet connection to another among the sources designated as being in the MultiWAN. Because the data flow is shared between multiple connections, the net effect is that the data load for each connection is reduced. This may be helpful if some of the connections involved in the MultiWAN have fixed data budgets.

The download and upload speeds for each source remain the same as they would if the connections were used individually, but the use of multiple connections results in more total data being able to flow in parallel across all connections. This can provide significant advantages when streaming video using connections as is explained in this article: https://wifiranger.com/how-load-balancing-makes-netflix-and-chill-better/

It should be noted that Load Balancing works best if all the connections used in the MultiWAN have roughly equivalent speed and response (ping) characteristics. A factor of two difference in connection speeds probably won't cause a noticeable effect, but a factor of 10 might.

All connections participating in a Load Balanced connection are pinged every 10 seconds. If the ping fails, the connection is then disconnected from the MultiWAN until a future ping to the same connection is successful. It should be noted that pinging does not verify speed of a connection, only its "existence".

It should be noted that Load Balancing may not work well with certain secure websites which may react poorly to what is perceived as a changing IP address for the user. If that is the case, simply disable the MultiWAN for those websites.

To create a Load Balanced MultiWAN connection, simply designate on the Setup tab which connections are to be included and save your selections. Then return to the Main tab and connect each of the designated connections. In the Internet box at the top center of the page, you will first see the text Configuring MultiWAN which will be followed by ONLINE with a list of the connections that are being used. Figure 5a-1 depicts a MultiWAN with two connections one of which uses the 2 GHz WiFi while the other is a cellular connection.

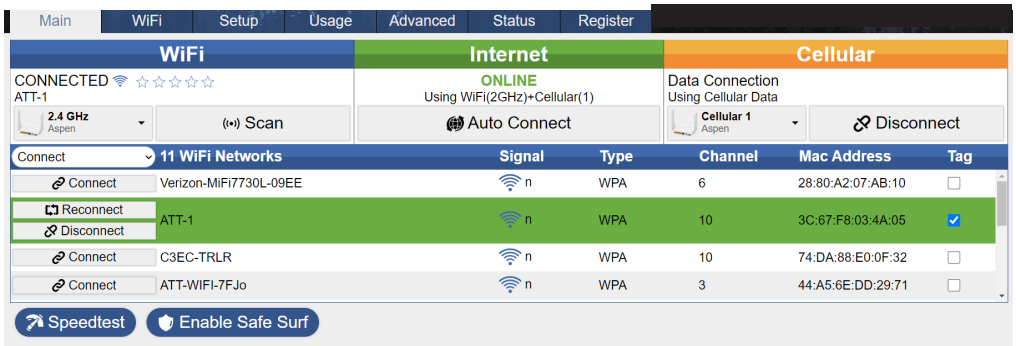

FIGURE 5a-1

5b HOT STANDBY MODE

In Hot Standby mode the Ranger will make “standby” connections to multiple internet sources but only one at a time will be in use. If the Ranger “senses” that its current connection has stalled, the data flow will automatically be shifted to the next connection in the MultiWAN. The “health” of a connection in a Hot Standby configuration is determined by pinging it every 10 seconds. As noted in the previous section, pinging doesn’t verify connection speed just that the connection is responding in a normal manner to a ping attempt.

In Hot Standby mode, connections will be accessed in the order in which they are listed in the top section of the Setup tab. The first listed connection in a Hot Standby MultiWAN is connected to using the Main tab of the control panel as usual. The second listed connection becomes the Standby connection, and the Ranger will so designate it with an orange “flame” icon next to it on the Main page of the control panel. Subsequent connections beyond the second will also become standbys.

All connections in a Hot Standby configuration will continue to be pinged every 10 sections, even if “data traffic” has been shifted to a secondary connection. This allows the system to transfer data flow back to a primary connection after the problems affecting it have been resolved.

Figure 5b-1 shows an example of a hot standby configuration where the WiFi connection is the primary with the standby being the cellular modem. Note that the cellular box displays “Data Connection” indicating that an active connection exists, but the “flame” icon on the right of the text shows that the connection is actually in standby mode.

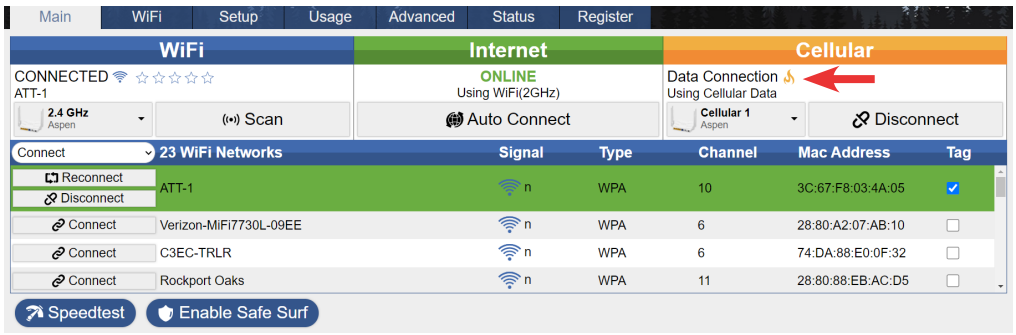

FIGURE 5b-1

6 GLOSSARY COMMON WIFI & CELLULAR TERMS

5G Fifth-generation wireless (5G) is the latest iteration of cellular technology, engineered to increase the speed and responsiveness of wireless networks.

ACCESS POINT (Also called a Wireless Access Point or WAP) In computer networking an access point is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

ETHERNET A standard communication protocol used to create local area networks. It transmits and receives data through cables.

FIRMWARE Permanent software programmed into a read-only memory in a device such as a router.

IP ADDRESS A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

LAN A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

LTE “Long Term Evolution”; the fourth generation cellular network standard.

MODEM A modem modulates and demodulates electrical signals sent through phone lines, coaxial cables, or other types of wiring; in other words, it transforms digital information from your computer into analog signals that can transmit over wires, and it can translate incoming analog signals back into digital data that your computer can understand.

NETWORK KEY Security key used to connect to a network; often called a password.

ROUTER A device which allows multiple devices to connect to and share an internet connection.

SPLASH SCREEN (FILTERED NETWORK) An initial screen displayed during a connection to a network; often found in commercial settings such as hotels, RV parks, restaurants, etc.

SSID A unique ID that consists of no more than 32 characters and is used for naming wireless networks (Stands for “Service Set Identifier”).

WAN Wide-area network as a computer network that connects smaller networks. Since WANs are not tied to a specific location, they allow localized networks to communicate with one another across great distances.

WIFI A family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves.

WPA, WPA2, WEP Encryption standards for WiFi communications.

7 INDEX