

Setup

Table of Contents

Section	Page	Section	Page
Introduction		Creating Another Security Association Database . . . 20	
Qualified Persons	2	Opening a Security Association Database 20	
Read this Instruction Sheet	2	Network Configuration 22	
Retain this Instruction Sheet.	2	Key Updater Tool 29	
Regulatory Information	3	SpeedNet Client Tool	
Warranty	4	Overview 33	
Warranty Qualifications.	4	Logging In 33	
Safety Information		Main Window. 34	
Understanding Safety-Alert Messages	5	Interfaces Window, Ethernet Tab 35	
Following Safety Instructions	5	Interfaces Window, Wireless Tab 37	
Replacement Instructions and Labels.	5	Interfaces Window, Serial Mode Tab 39	
Safety Precautions 6		Multiple SCADA Masters. 41	
Network Setup		Repeater/SpeedGate Serial Gate Mode 41	
Overview	7	Interfaces Window, Serial Port Tab 42	
SpeedNet Security Administration		Serial Pass-Through 43	
SpeedNet Security Information	9	IP Routing Window, Ad Hoc Routing Tab. 44	
KeyGen Utility	9	IP Routing Window, Routes Tab 48	
Creating a Security Association Database	9	IP Routing Window, ARP Tab 49	
User Management Window.	10	IP Routing Window, Blacklist Tab 50	
Adding a User	11	Security Window, Encryption Tab 51	
Deleting a User	12	Security Window, MAC Filter Tab 52	
Modifying a User	12	Admin Window, System Tab 53	
Clearing All Users	13	Admin Window, Firmware Tab 54	
Adding a MAC Address to the Revocation List	13	Admin Window, Shell Tab 54	
Deleting a MAC Address from the Revocation List	14	Statistics Window, Ethernet Tab 56	
Clearing the Revocation List	14	Statistics Window, ICMP Tab 57	
Key Generation	15	Statistics Window, UDP Tab 58	
Adding a Keypset	15	Statistics Window, IP Tab 58	
Deleting a Keypset	16	Statistics Window, Wireless Tab 60	
Generating a Security File	17	Statistics Window, Battery Status Tab 60	
Saving a Security Association Database.	19	Statistics Window, AODV Tab 62	
		Statistics Window, RSSI Tab 62	



NOTICE

SpeedNet Radio software and instruction sheets can be downloaded at sandc.com/support/automation-customer-support-portal.asp If you need assistance, please contact customerportal@sandc.com or call (800) 621-5546.



Qualified Persons

⚠ WARNING

The equipment covered by this publication must be installed, operated, and maintained by qualified persons who are knowledgeable in the installation, operation, and maintenance of radios in electric power distribution equipment, along with the associated hazards. A qualified person is a radio technician who is qualified to install transmission-power-limited radio equipment per FCC Part 15 and who is trained and competent in:

- The skills and techniques necessary to distinguish exposed live parts from nonlive parts of electrical equipment
- The skills and techniques necessary to determine the proper approach distances corresponding to the voltages to which the qualified person will be exposed
- The proper use of the special precautionary techniques, personal protective equipment, insulating and shielding materials, and insulated tools for working on or near exposed energized parts of electrical equipment

These instructions are intended only for such qualified persons. They are not intended to be a substitute for adequate training and experience in safety procedures for this type of equipment.

Read this Instruction Sheet

NOTICE

Thoroughly and carefully read this instruction sheet before programming, operating, or maintaining your S&C SpeedNet Radios. Familiarize yourself with the Safety Information and Safety Precautions on pages 5 and 6. The latest version is available online in PDF format at sandc.com/Support/Product-Literature.asp

These instructions apply to SpeedNet Radio Firmware Version v2.5.3. The version number can be found on the **Admin>System** window of the SpeedNet Client Tool version 2.5.3, as shown in Figure 1.

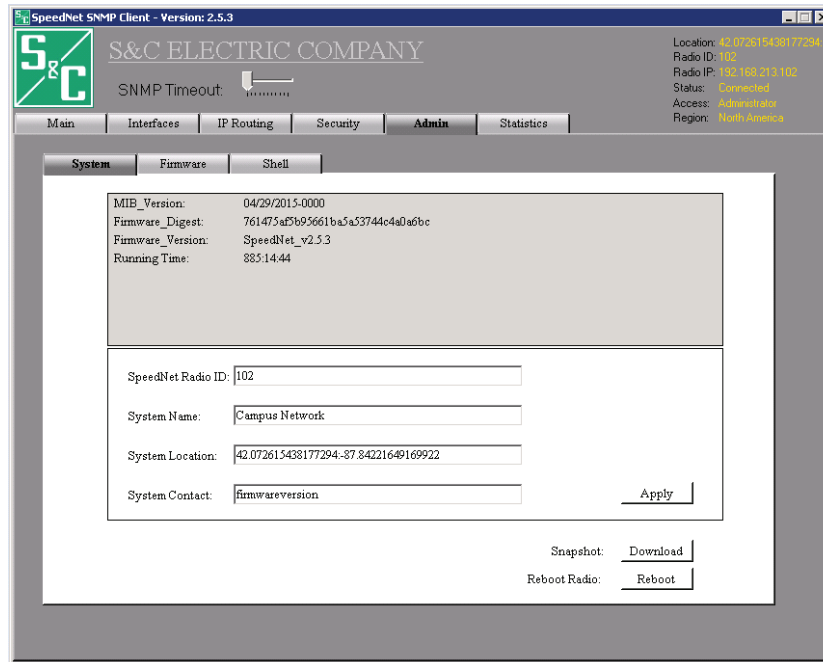


Figure 1. Admin>System window in the SpeedNet Client Tool

Retain this Instruction Sheet

This instruction sheet should be available for reference wherever SpeedNet Radio is to be used. Retain this instruction sheet in a location where you can easily retrieve and refer to it.

Regulatory Information

This device complies with part 15 of the FCC rules and regulations regarding unlicensed transmissions. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference.

This device complies with Industry Canada license exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme avec Industrie Canada exempts de licence(s) standard RSS. Son fonctionnement est soumis aux deux conditions suivantes: (1) ce dispositif ne doit pas causer d'interférences, et (2) cet appareil doit accepter toute interférence, y compris celles pouvant causer un mauvais fonctionnement de l'appareil.

FCC Warning

This device must be professionally installed. It is the responsibility of the installer to ensure that proper antenna and cable combinations are used in order to remain within FCC Part 15 limits.

The SpeedNet Radio is specifically designed to close the longest possible links. This goal is accomplished in part by delivering the highest permissible RF output power to the antenna per the FCC Part 15 Rules. In August 1996, the FCC adopted RF exposure guidelines that established safety levels for various categories of wireless transceivers. Those limits are consistent with safety standards previously published by the National Council on Radiation Protection (NCRP) Report 86, §17.4.1, §17.4.1.1, §17.4.2, and §17.4.3 as well as the American National Standards Institute (ANSI) in §4.1 of "IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 30 GHz," ANSI/IEEE C95.1-1992.

The SpeedNet Radio complies with these FCC exposure guidelines when the following precautions are obeyed:

- One of the exact antennas recommended in this instruction sheet is installed
- The cable run for the selected antenna exceeds the minimum length quoted in this instruction sheet
- All persons maintain a minimum separation of 12 inches (30.48 cm) from the SpeedNet antenna

Disconnect the ac/dc input power source from the SpeedNet Radio whenever repositioning the antenna. You are responsible for taking the necessary steps to ensure that these guidelines are communicated to all persons that may come near the SpeedNet Radio antenna.

NOTICE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by using 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

CAN ICES-3 (B)/NMB-3(B)

NOTICE

Changes or modifications not expressly approved by S&C Electric Company could void the user's authority to operate the equipment.

Warranty

The standard warranty contained in S&C's standard conditions of sale, as set forth in Price Sheet 150, applies to S&C SpeedNet Radios.

Warranty Qualifications


Warranty of the SpeedNet Radio is contingent upon the installation, configuration, and use of the SpeedNet Radio and software in accordance with S&C's applicable instruction sheets. This warranty does not apply to major components not of S&C manufacture, such as batteries, and other communication devices not of S&C manufacture. However, S&C will assign to the immediate purchaser or end user all manufacturers' warranties that apply to such major components.

**Understanding
Safety-Alert Messages**

Several types of safety-alert messages may appear throughout this instruction sheet as well as on labels attached to the SpeedNet Radio. Familiarize yourself with these types of messages and the importance of these various signal words:

 DANGER
“DANGER” identifies the most serious and immediate hazards that <i>will</i> likely result in serious personal injury or death if instructions, including recommended precautions, are not followed.


 WARNING
“WARNING” identifies hazards or unsafe practices that <i>can</i> result in serious personal injury or death if instructions, including recommended precautions, are not followed.

 CAUTION
“CAUTION” identifies hazards or unsafe practices that <i>can</i> result in minor personal injury if instructions, including recommended precautions, are not followed.

NOTICE
“NOTICE” identifies important procedures or requirements that <i>can</i> result in product or property damage if instructions are not followed.

**Following Safety
Instructions**

If you do not understand any portion of this instruction sheet and need assistance, contact your nearest S&C Sales Office or S&C Authorized Distributor. Their telephone numbers are listed on S&C’s website **sandc.com**. Or call S&C Headquarters at (773) 338-1000; in Canada, call S&C Electric Canada Ltd. at (416) 249-9171.

NOTICE	
Read this instruction sheet thoroughly and carefully before installing or operating your S&C SpeedNet Radio.	

**Replacement
Instructions and
Labels**

If you need additional copies of this instruction sheet, contact your nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

It is important that any missing, damaged, or faded labels on the equipment be replaced immediately. Replacement labels are available by contacting your nearest S&C Sales Office, S&C Authorized Distributor, S&C Headquarters, or S&C Electric Canada Ltd.

DANGER



SpeedNet Radios operate between +9 and +36 Vdc. Failure to observe the precautions below will result in serious personal injury or death.

Some of these precautions may differ from your company's operating procedures and rules. Where a discrepancy exists, follow your company's operating procedures and rules.

1. **QUALIFIED PERSONS.** Access to an SpeedNet Radio must be restricted only to qualified persons. See "Qualified Persons" on page 2.
2. **SAFETY PROCEDURES.** Always follow safe operating procedures and rules.
3. **PERSONAL PROTECTIVE EQUIPMENT.** Always use suitable protective equipment such as rubber gloves, rubber mats, hard hats, safety glasses, and flash clothing, in accordance with safe operating procedures and rules.
4. **SAFETY LABELS.** Do not remove or obscure any of the "DANGER," "WARNING," "CAUTION," or "NOTICE" labels.
5. **SAFE DISTANCE.**
 - All persons should maintain a minimum separation of 12 inches (30.48 cm) for the SpeedNet antenna.
 - Disconnect the ac/dc input power source from the SpeedNet Radio whenever configuring or repositioning the antenna.
9. **MAINTAINING PROPER CLEARANCE.** Always maintain proper clearance from energized components.

Overview

SpeedNet Radios are versatile, smart grid-enabled wireless devices designed specifically for power distribution automation, SCADA, and AMI Backhaul communications. SpeedNet Radios provide wireless connections between two or more Internet Protocol (IP) or serial devices. Application devices, such as the S&C IntelliRupter® PulseCloser® Fault Interrupter, can be connected to a SpeedNet Radio. As routers, SpeedNet Radios route IP data between separate Ethernet subnets. Data are routed between the Ethernet subnets over a common IP-based wireless network. Route information can be entered manually, or it can be handled automatically by the SpeedNet Radio's proprietary enhanced version of the Ad hoc On demand Distance Vector (AODV) routing protocol.

AODV is a routing protocol for mobile ad hoc networks and other wireless ad hoc networks. SpeedNet Radios use a proprietary AODV routing system that works dynamically to maintain message routing. It generates fewer transmissions and conserves network capacity.

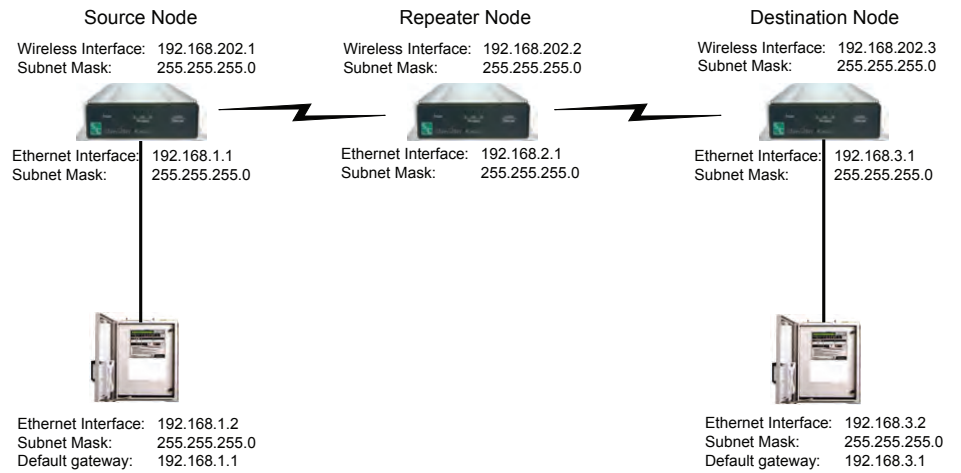


Figure 2. A multi-node SpeedNet network.

The SpeedNet Radio network depicted in Figure 2 on page 7 contains three Ethernet segments. The first segment uses the 192.168.1.0 Class C subnet that encompasses a range of addresses from 192.168.1.1 to 192.168.1.254. The second segment uses the 192.168.2.0 Class C subnet that encompasses a range of addresses from 192.168.2.1 to 192.168.2.254. The third segment uses the 192.168.3.0 Class C subnet that encompasses a range of addresses from 192.168.3.1 to 192.168.3.254.

The wireless network shown in Figure 2 uses the 192.168.202.0 Class C subnet. This subnet is different from the subnets used for the Ethernet segments. The wireless interface of the SpeedNet Radio from the Source Node 1 is assigned an address of 192.168.202.1. The wireless interface of the SpeedNet Radio from the repeater node is assigned an address of 192.168.202.2. The wireless interface of the SpeedNet Radio from Destination Node 2 is assigned an address of 192.168.202.3.

In Figure 2, each SpeedNet Radio host ID is 1 (as in 192.168.3.1), while the connected application device uses a host ID of 2 (as in 192.168.3.2). Following a numbering scheme such as this will make it easier to keep track of which IP addresses are assigned to each device.

NOTE: All SpeedNet Radios, regardless of their role within the network, must use unique IP addresses for their Ethernet and wireless interfaces. All the SpeedNet Radios on the same mesh should have wireless IP addresses in the same subnet. All the SpeedNet Radios on the same mesh should have different Ethernet subnets.

Refer to S&C Instruction Sheet 1072-510 for additional information about network planning.

SpeedNet Security Information

SpeedNet Radios use a comprehensive security suite to prevent unauthorized network access and to protect sensitive data. The security features include user access controls, network data encryption, node access revocation, and anti-spoofing measures. These security features should be incorporated as part of a complete security policy, which should include application-level user authentication and stringent password policies. One example would be a security policy requiring user-password changes at a defined interval.

KeyGen Utility

Administrative control of SpeedNet Radio security configuration is provided by the SpeedNet KeyGen Utility, an application that generates security keys, updates user access and radio revocation lists, and saves updated security profiles within a Security Association Database (SAD). The KeyGen Utility also allows generation of a common configuration file to load into multiple radios, easing configuration overhead.

Creating a Security Association Database

Use the following procedure to create a security association database:

STEP 1. Launch the KeyGen application. The **Launch** window will open. See Figure 3.

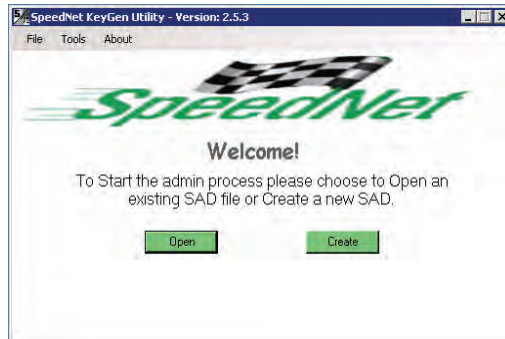


Figure 3. The KeyGen application launch window.

STEP 2. Click the **Create** button to create a Security Association Database (SAD). The SAD dialog box will open. See Figure 4.

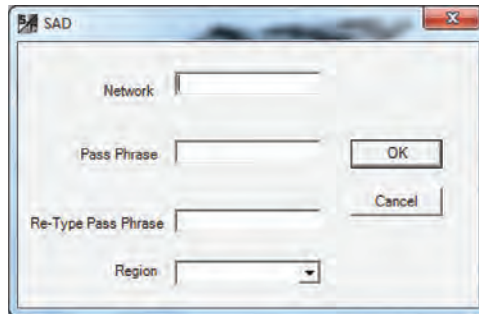


Figure 4. The Security Association Database dialog box.

NOTICE

The Security Association Database, stored in a .sad file, is encrypted and protected by the network name and pass phrase combination specified at the creation of the database. Loss of the network name and pass phrase combination means the Security Association Database becomes unusable. This may imply a new database would need to be created. Also, all radios would need to be reset to factory settings and re-programmed with security files derived from a new database. As such, it is vital to keep track of the network name and pass phrase credentials associated with the database.

- STEP 3.** Enter a network name that is 4 to 64 characters in length. Use the Tab key on your keyboard to proceed to the next field.
- STEP 4.** Enter a pass phrase that is 8 to 64 characters in length. Use the Tab key on your keyboard to proceed to the next field.
- STEP 5.** Retype the pass phrase to confirm the previously entered pass phrase.
- STEP 6.** Select a region from the drop down list. Then click the **OK** button.
- STEP 7.** Save the Security Association Database file as a .sad file. See Figure 5. The **User Management** window will open. See Figure 6.

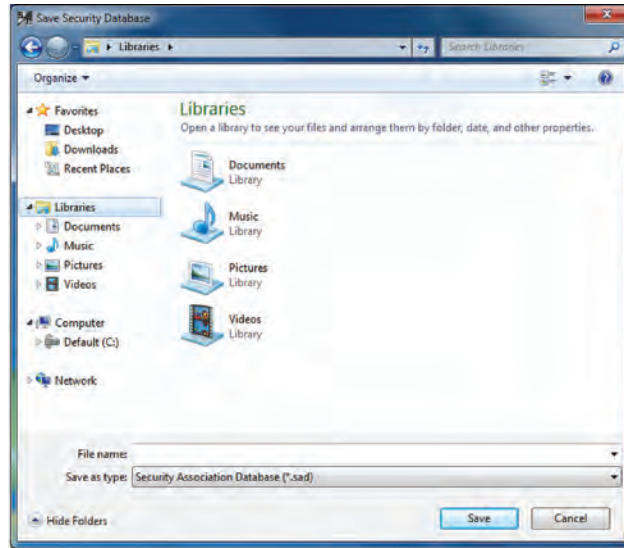


Figure 5. The Security Association Database save dialog box.

User Management Window

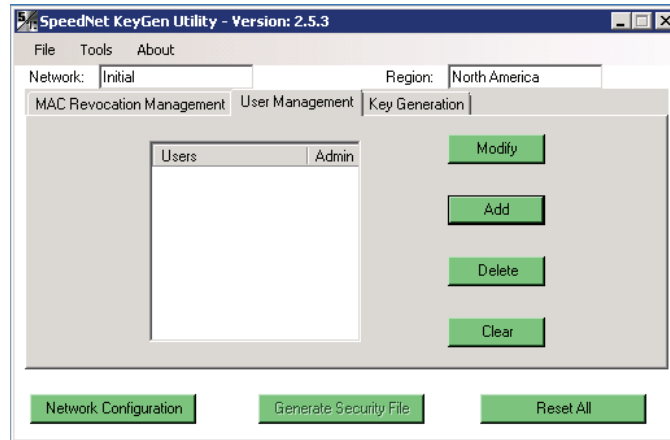


Figure 6. The KeyGen User Management window.

The User Management window allows the administrator to add up to six users to the system. Any users with a check mark entered in the Admin column will have full security access. Users created without this checkmark entered have limited, read-only privileges when accessing the radios. Admin-level access is required to configure the radios.

Adding a User

Follow this process to manage users:

- STEP 8.** Click the **Add** button on the **User Management** window. The User File dialog box will open. See Figure 7.

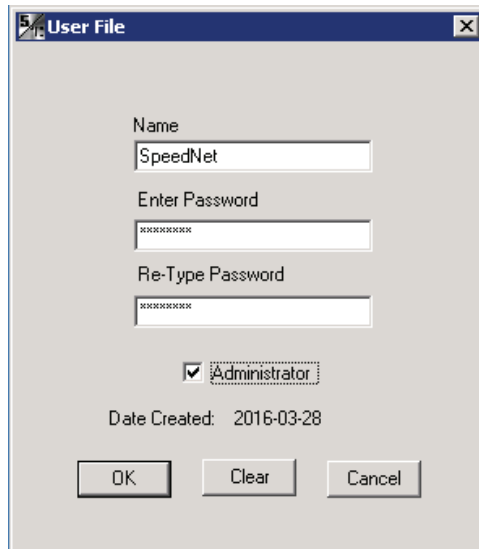


Figure 7. The KeyGen User File dialog box.

- STEP 9.** Enter a user name that is 8 to 16 characters in length. Valid case-sensitive characters are a-z, A-Z, and 0-9. Use the Tab key on your keyboard to proceed to the next field.
- STEP 10.** Enter a password that is 8 to 16 characters in length. Valid case-sensitive characters are a-z, A-Z, and 0-9. Use the Tab key on your keyboard to proceed to the next field.
- STEP 11.** Retype the password to confirm the previously entered password. Click to check the **Administrator** checkbox if the user will be an administrator. Click the **OK** button. See Figure 7.

The newly added user will appear in the **KeyGen User Management** window. See Figure 8.

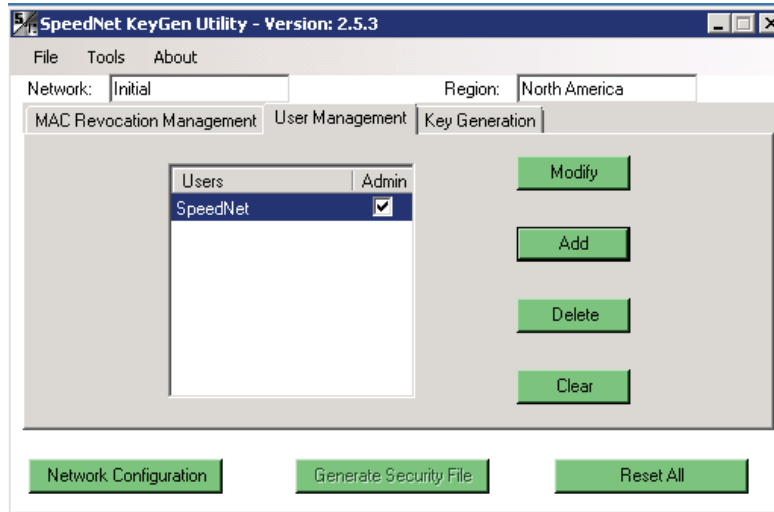


Figure 8. Adding a KeyGen user.

Deleting a User

- STEP 12.** To delete a user from the users list, highlight that user’s name. Then click the **Delete** button. See Figure 9.

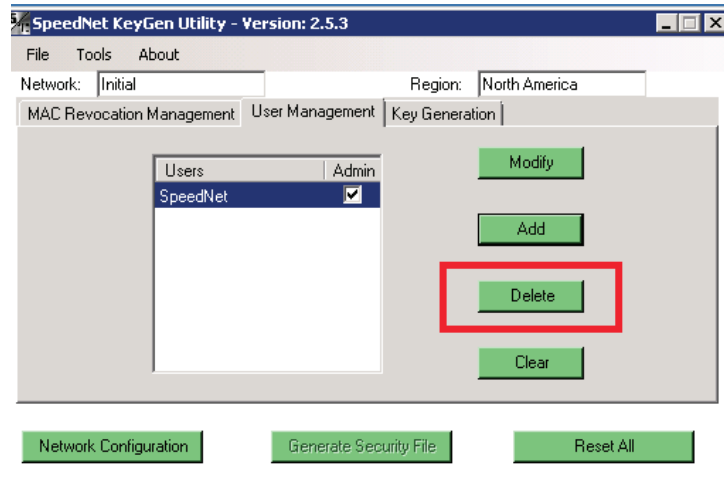


Figure 9. The KeyGen User Management window Delete button.

The User Management dialog box will open. See Figure 10.

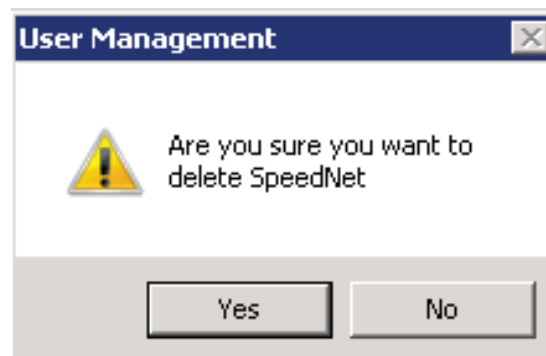


Figure 10. The User Management dialog box.

STEP 13. Click the **Yes** button to delete the selected user from the user list.

Modifying a User

STEP 14. To modify a user name and/or password, first select the user from the User Management list. Then click the **Modify** button. See Figure 11.

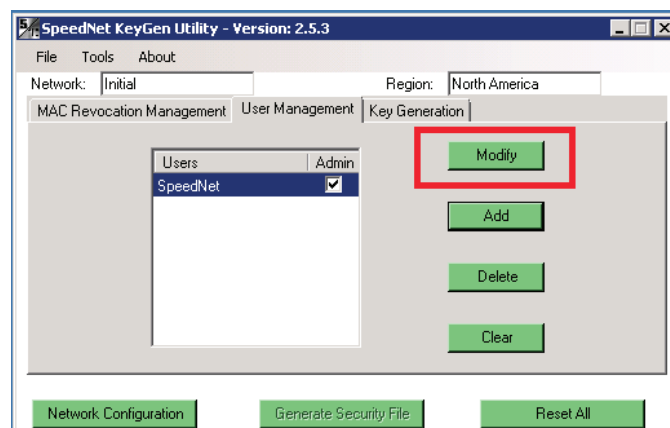


Figure 11. The KeyGen User Management window.

The User File dialog box will open that includes user details. See Figure 12.

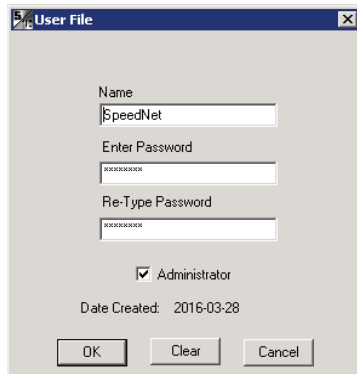


Figure 12. The KegGen User File dialog box.

Clearing All Users

STEP 15. To clear all users click the **Clear** button on the **User Management** window. The **User Management** confirmation dialog box will be displayed. See Figure 13.

STEP 16. Make the appropriate changes. Then click the **OK** button.

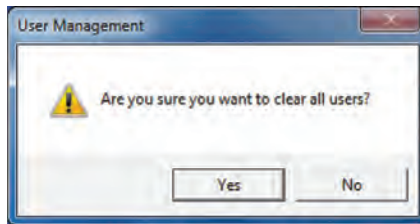


Figure 13. User Management dialog box.

STEP 17. Click the **Yes** button to delete all users from the User Management list. Further radio management will require at least one admin account and a person possessing that account's login credentials (username and password).

Adding a MAC Address to the Revocation List

The **Mac Revocation Management** window is used to update the revocation list for the Media Access Control (MAC) address filter. See Figure 14. The MAC address is factory-programmed into SpeedNet Radios. As such, revoking a MAC address is a means to exclude radios. For example, if a SpeedNet Radio were stolen, it would be wise to exclude that radio's MAC address as one means to prevent the radio from joining a mesh and breaching SpeedNet Radio network security.

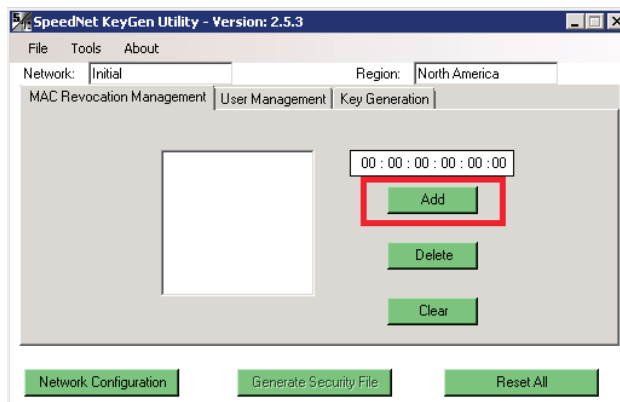


Figure 14. The MAC Revocation Management window.

To add a new MAC address to the revocation list, switch to the **MAC Revocation Management** window. Enter the MAC address of the SpeedNet Radio to be excluded from communicating with the radio being configured. The valid hexadecimal characters are a-f and 0-9. Click the **Add** button.

Deleting a MAC Address from the Revocation List

To delete a MAC address from the revocation list, highlight the address on the **MAC Revocation Management** window. Click the **Delete** button. See Figure 15.

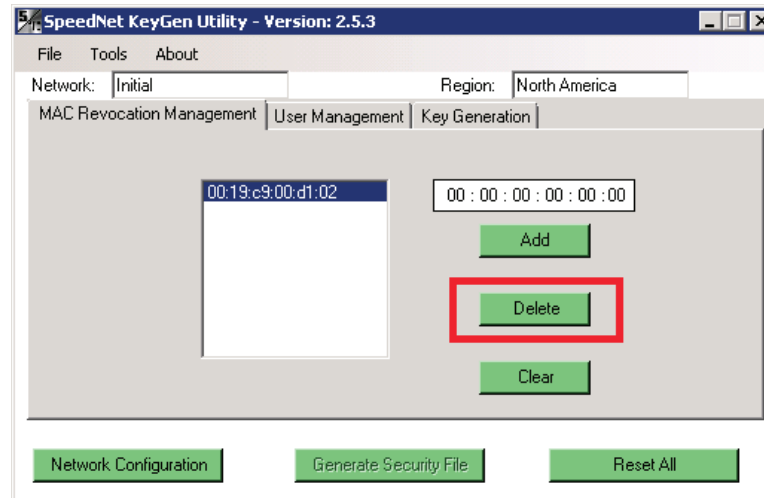


Figure 15. The MAC Revocation Management window.

The **Mac Management** dialog box will be displayed. See Figure 16.

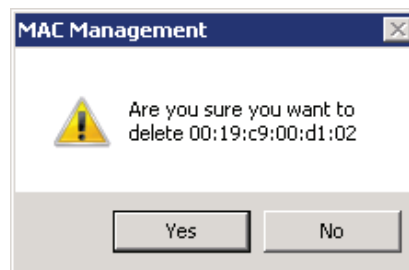


Figure 16. The Mac Management dialog box.

Click the **Yes** button to delete the MAC address.

Clearing the Revocation List

To clear all addresses, click the **Clear** button on the **MAC Revocation Management** window. See Figure 17.

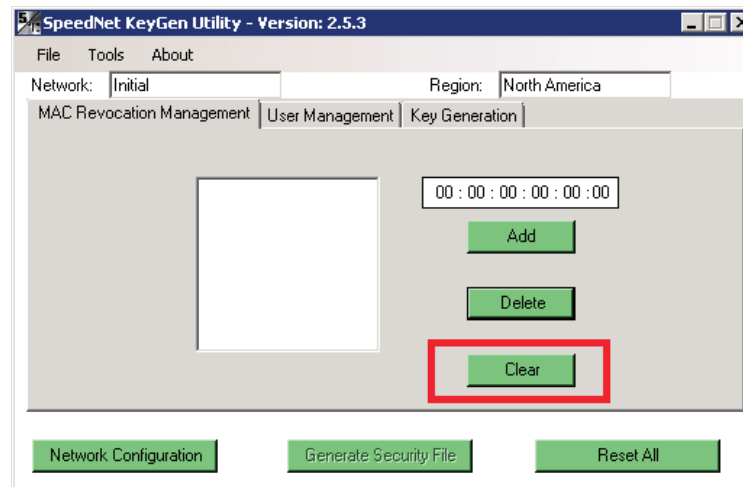


Figure 17. The MAC Revocation Management window.

The **MAC Management** dialog box will open. See Figure 18.

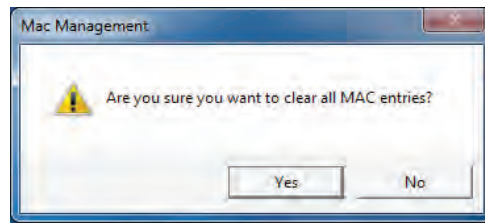


Figure 18. The Clear all MAC entries dialog box.

Click the **Yes** button to clear the Mac Revocation list.

Key Generation

The keyset is a common credential all radios use when optionally encrypting UDP/IP and TCP/IP data over a SpeedNet network. Keysets are thus used when AES 128-bit encryption is enabled (SpeedNet Client tools' **Security**>**Encryption** tab using the **Enable Encryption** check box). Keysets must be installed on all participating radios to be available for use; it is not sufficient to merely generate them in the KeyGen tool. The KeyGen tool generates keysets randomly without user input; the user does not provide seeds or other data. The **Key Generation** window is used to update keysets. For a network or security configuration to be applied to the radio, the configuration file must be encrypted and authenticated with a current keyset. Up to six keysets can be loaded into a radio at a given time. At most one keyset is active at any given time. Radios can "roll forward" to new keysets upon prompting by users or when data of a newer keyset is received from another radio. Radios do not "roll backward" to previous keysets.

Adding a Keyset

To add a new keyset, open the **Key Generation** tab and click the **Add Keyset** button. See Figure 19.

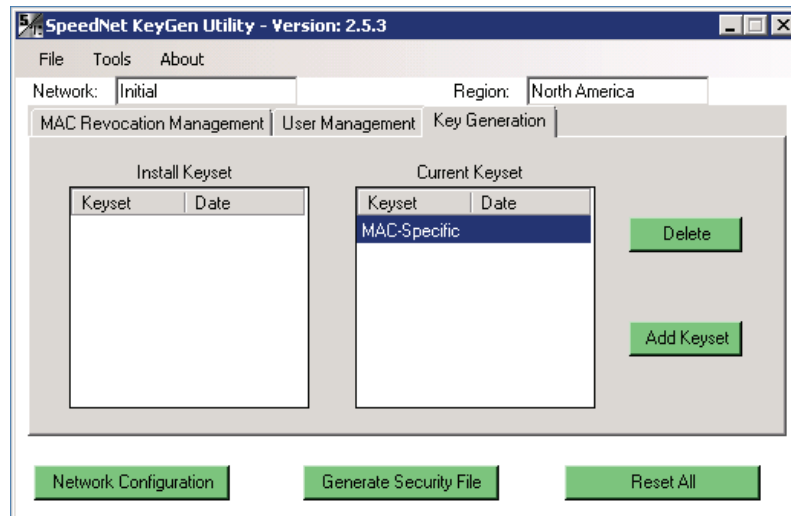


Figure 19. The Key Generation window.

Each time the **Add Keyset** button is clicked, the next consecutive keyset number will be automatically added to the Install Keyset list as shown in Figure 20 on page 16.

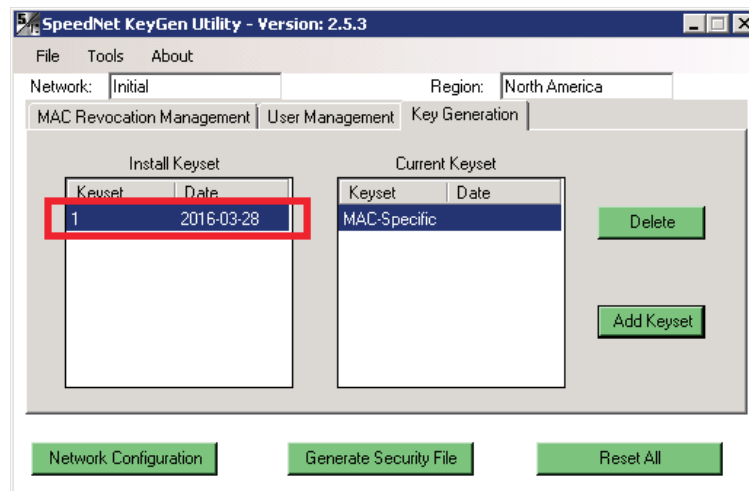


Figure 20. New keyset number is available on the Install Keyset list.

Deleting a Keyset

To delete a keyset, open the **Key Generation** tab and highlight the keyset. Then click the **Delete** button. See Figure 21.

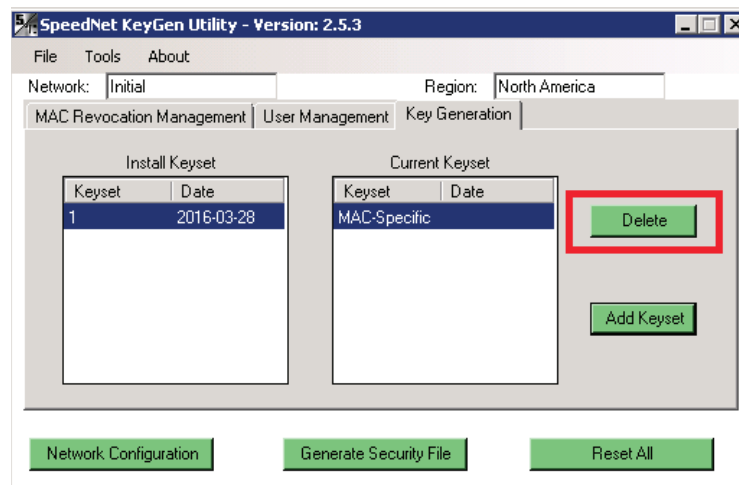


Figure 21. The Key Generation window.

The confirmation dialog will open. See Figure 22. Click the **Yes** button to delete the keyset.

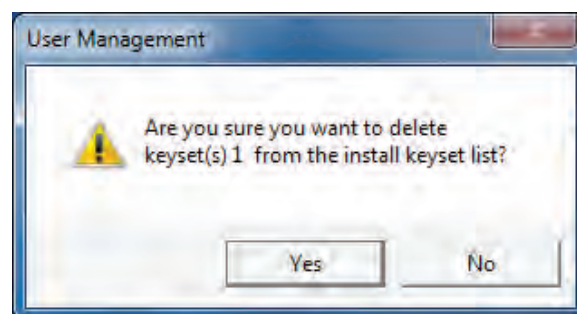


Figure 22. The Delete keyset(s) confirmation dialog box.

NOTICE

The current keyset list will not be updated until a new security file is generated. Security configuration files can still be encrypted to a recently deleted keyset because the old keyset is still stored in the current keyset list. If, after deleting a keyset, you add a keyset with the same tag as the deleted keyset, the keyset in the Install Keyset list will contain a different key than the keyset with the same tag in the current keyset list. Care must be taken to avoid this because all radios must have the same keyset installed to communicate UDP/IP and TCP/IP data. ICMP data used for pings is not encrypted in SpeedNet radios, so pings may work even in the case of mismatched keysets on radios with encryption enabled. SpeedNet Client Tool logins use SNMPv3, which is transported over UDP/IP, so logins will not work over wireless links in the case of mismatched keysets on radios with encryption enabled.

Generating a Security File

Follow this process to generate a security file:

STEP 18. Select up to six keysets from the installed Keyset list.

STEP 19. Click the **Generate Security File** button on the **Key Generation** window. The **Security File** window will open with all selections listed. See Figure 23.

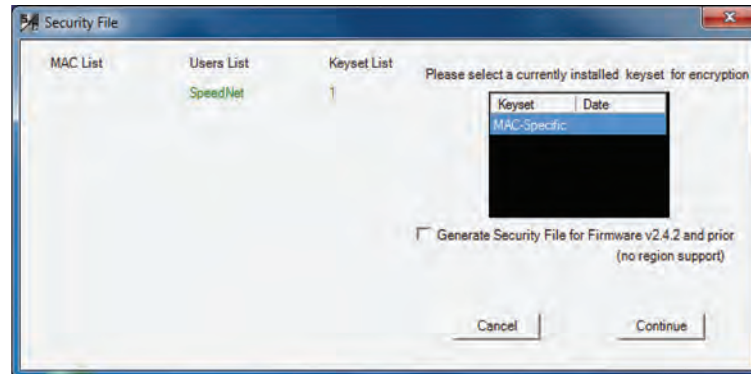


Figure 23. The Security File window.

STEP 20. Verify all the data to be included and select a current keyset to encrypt the file. Click the **Continue** button. If a MAC-specific key is used to encrypt the file, the dialog box shown in Figure 24 will be displayed.

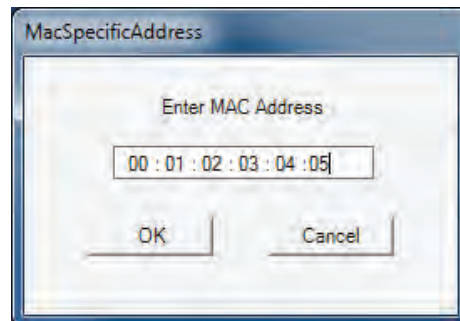


Figure 24. The Enter Mac Address dialog box.

STEP 21. Enter the MAC address of the radio for which this file is intended and then click the **OK** button.

STEP 22. Enter a file name for the security file. See Figure 25 on page 18. Then click the **Save** button. It's good practice to use the MAC address of the target radio as the filename or as part of the filename for the security file.

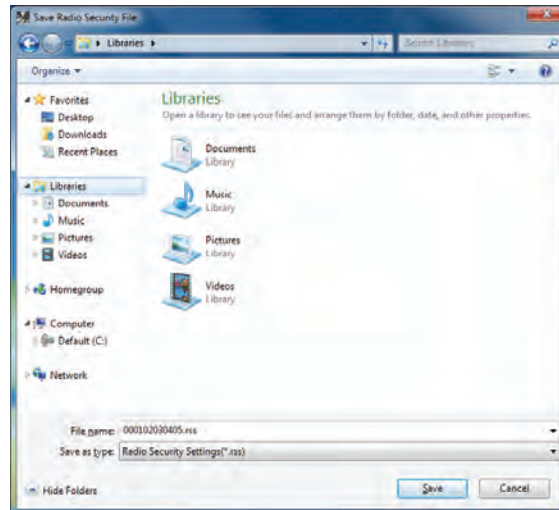


Figure 25. The Save Radio Security File dialog box.

After the security file is generated, the current keyset list will be updated with all of the installed keysets, as shown in Figure 26.

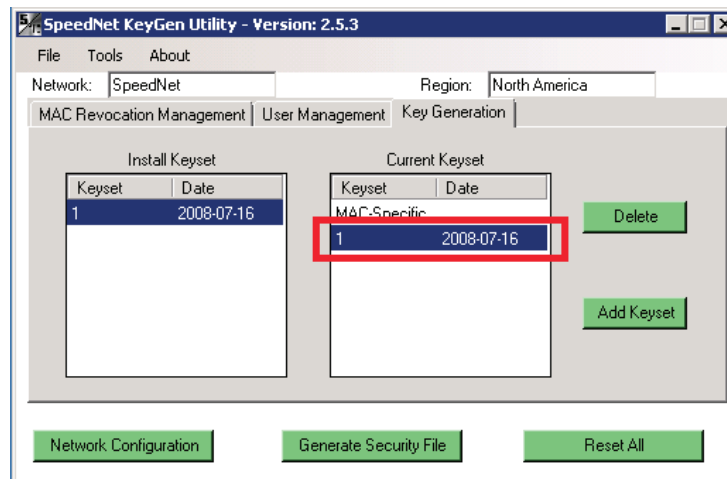


Figure 26. Updated Current Keyset list in the dialog box.

The maximum number of keyset tags allowed is 63. If you attempt to add another keyset after 63 keyset tags have been entered, the dialog box shown in Figure 27 will be displayed requesting permission to overwrite an existing keyset.

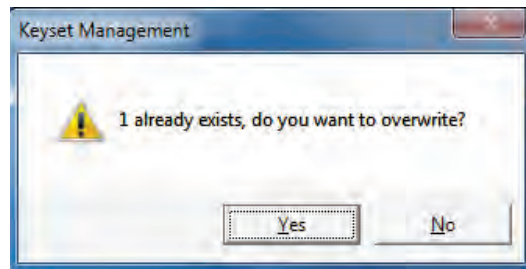


Figure 27. Dialog box requesting permission to overwrite an existing keyset.

STEP 23. Click the **Yes** button to overwrite Keyset 1.

To delete a specific keyset, highlight the keyset (the example in Figure 28 on page 19 is Keyset 59). Click the **Delete** button.

Saving a Security Association Database

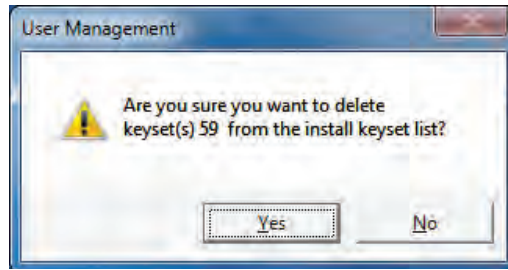


Figure 28. Dialog box requesting permission to delete a keyset.

STEP 24. Click the **Yes** button to delete Keyset 59.

The deleted keyset will not be deleted from the Current Keyset list until a new security file is generated.

Follow this process to save an SAD file:

STEP 25. Open the **File** menu in the upper-left corner of the **SpeedNet KeyGen Utility** window. Scroll down and select **Save**. See Figure 29.

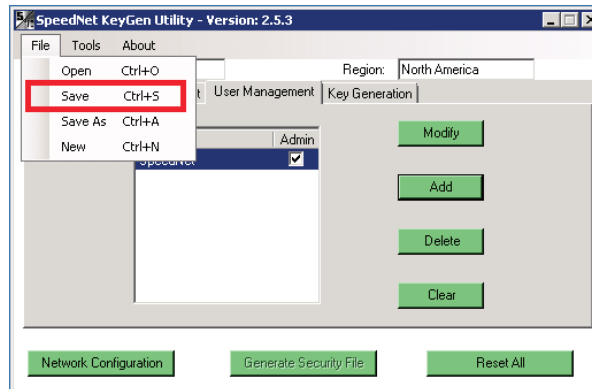


Figure 29. The SpeedNet KeyGen Utility window save SAD.

STEP 26. The **Save Security Database** window will open. See Figure 30. Enter a file name for the database, and click the **Save** button.

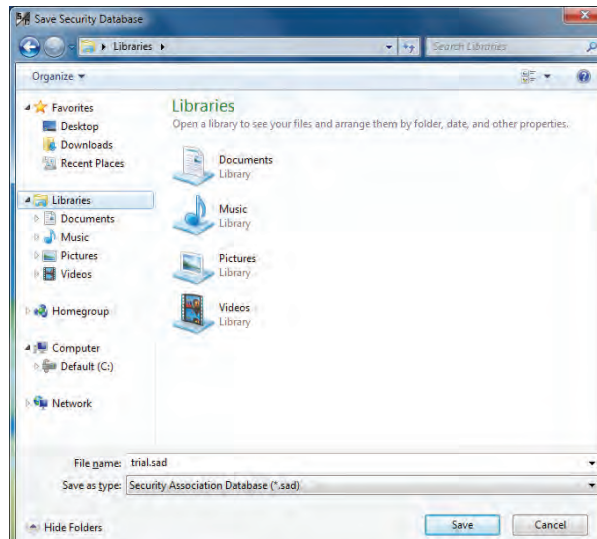


Figure 30. The Save Security Database window.

The database will be encrypted with the pass phrase that was provided when the SAD was created. It is important to retain the pass phrase and network name to preserve access to the security information for the radios.

Creating Another Security Association Database

Open the **File** menu in the upper-left corner of the **SpeedNet KeyGen Utility** window. Scroll down and select **New**. See Figure 31.

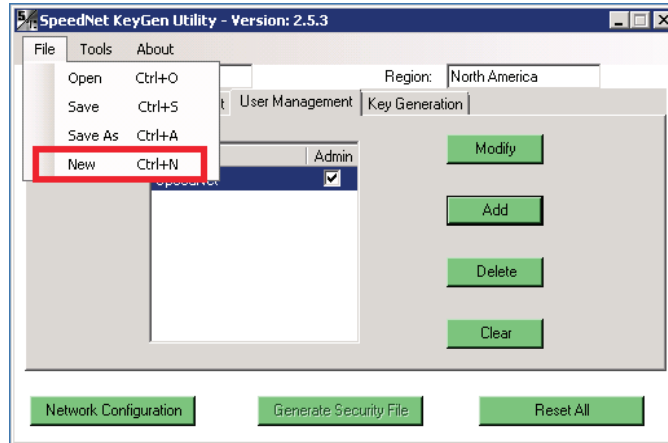


Figure 31. SpeedNet KeyGen Utility window for selecting a new SAD.

The new **SAD** window will open with all entries cleared.

Opening a Security Association Database

Follow this process to open an SAD file:

STEP 27. Open the **File** menu in the upper-left corner of the **SpeedNet KeyGen Utility** window. Scroll down and select **Open**. See Figure 32.

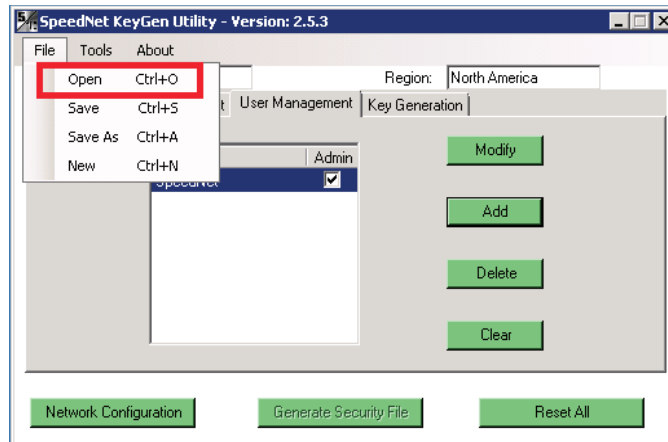


Figure 32. SpeedNet KeyGen Utility window to open a SAD.

STEP 28. The **Open Security Database** window will open. See Figure 33 on page 21. Enter the file name of the SAD database, and click the **Open** button.

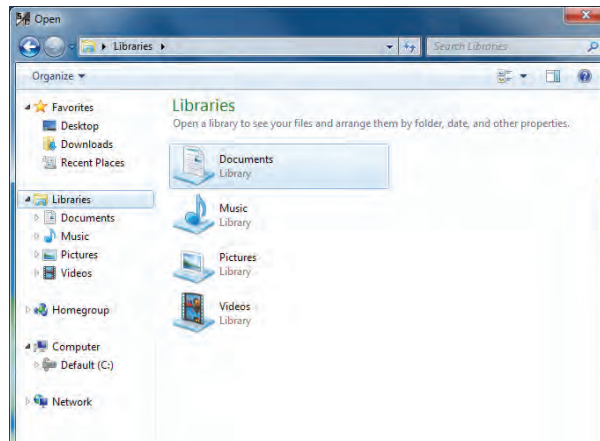


Figure 33. The Open Security Database window.

The SAD dialog box will open. See Figure 34.

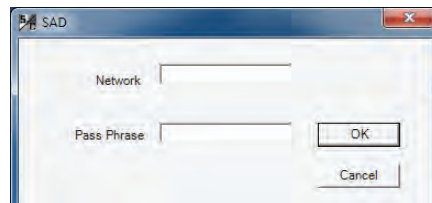


Figure 34. The SAD dialog box.

STEP 29. Enter the network name and pass phrase, and click the **OK** button.

NOTICE

The SAD is encrypted with a key derived from the pass phrase. If you forget the pass phrase used when you created the SAD, data in the SAD will not be accessible and will therefore be lost. There is no back door or other key recovery method. To update secured radios without a valid SAD, you will first need to return them to the factory default configuration.

Once the SAD file is open, the configuration can be edited by opening the **Tools** menu at the top of the window. See Figure 35. Select **Configuration**, or simply click the **Network Configuration** button located at the bottom of the **SpeedNet KeyGen Utility** window.

The SpeedNet KeyGen Utility will open the **Main** window shown in Figure 36 on page 22.

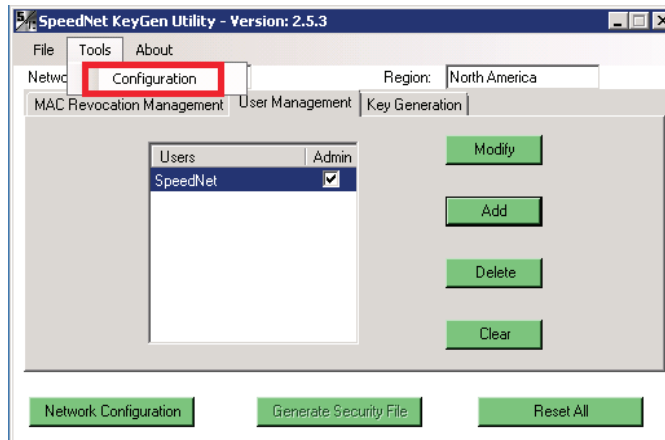


Figure 35. The SpeedNet KeyGen Utility—Network Configuration button.

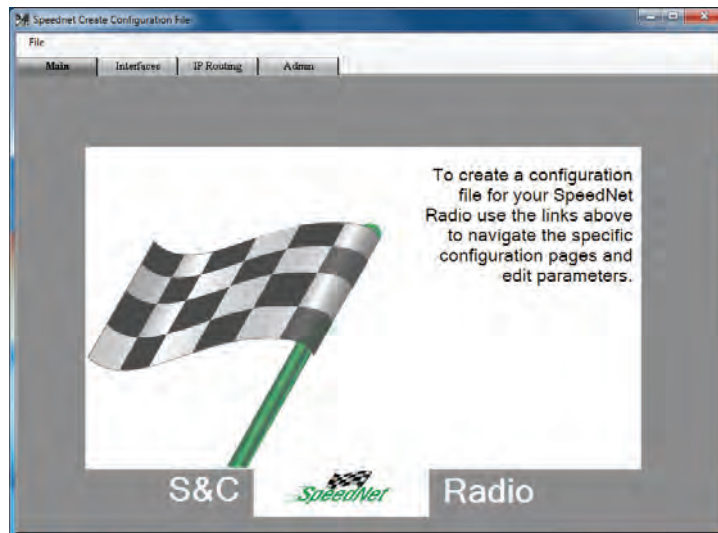


Figure 36. SpeedNet Network Configuration Main Window.

The File menu allows the following functionalities:

- **Open**—Opens an existing network configuration
- **Save**—Saves the current working network configuration.
- **Save As**—Edits the file name before saving
- **Reset to Defaults**—Restores the current working network configuration to factory default values

When opening a network configuration file, the window shown in Figure 37 will open and list all currently installed keysets. Select the keyset that was used to encrypt the file. Click the **Continue** button. The data from the file will be displayed in the configuration dialog. When saving a file, the same window will prompt you for the keyset to use to encrypt the file.



Figure 37. The Configuration File Keyset selection window.

The dialog shown in Figure 38 will open when a MAC-specific key is used to encrypt or decrypt the configuration file. A network-configuration file should only be encrypted with a MAC address once when the radio is initially deployed. If the radio has already been deployed, use a different encryption/decryption key.

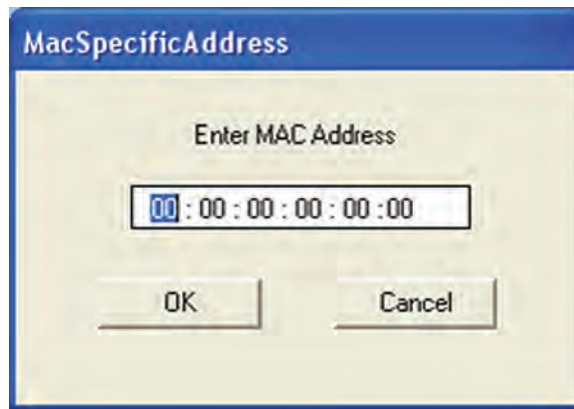


Figure 38. Configuration File MAC Address specification for MAC-specific encryption/decryption.

Configuration files are always encrypted to prevent tampering with radio configuration and to prevent snooping radio configurations during configuration uploads. When a keyset is used to encrypt/decrypt the configuration, the target radio must have that same keyset loaded to successfully upload and implement the network configuration.

Click on any of the tabs shown in Figure 36 on page 22 to set up the network configuration for the area listed in that tab. Network-configuration functions parallel the corresponding tabs in the SpeedNet Client Tool, but instead of applying to the radio the client is connected to, the settings developed in the network configuration are saved in a file that can be uploaded and applied to the corresponding radio by using the client tool's **Set Network Configuration** function described in the “Security Window, Encryption Tab” section on page 51.

The network configuration areas are described in Figure 39.

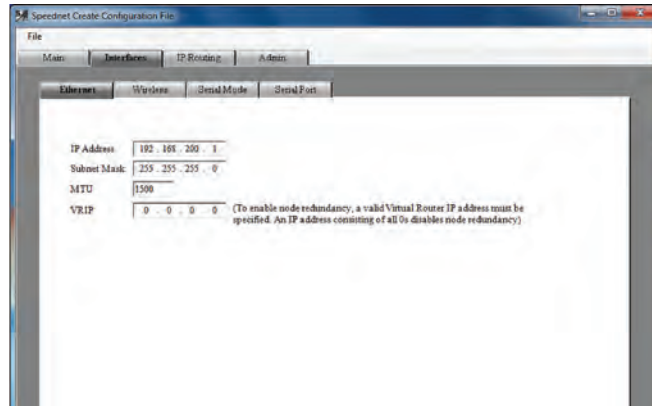


Figure 39. The Network Configuration of Ethernet Interface.

Figure 39 shows the **Network Configuration** window for configuring the Ethernet Interface. The IP Address, Subnet Mask, MTU, and VRIP settings function the same as in the corresponding **SpeedNet Client** window as described in the “Interfaces Window, Ethernet Tab” section starting on page 35. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

Please note that on a given SpeedNet Radio mesh, the configurations of all the Ethernet interfaces should differ so there is no overlap between the Ethernet port subnets or between the Ethernet port subnets and the wireless subnet.

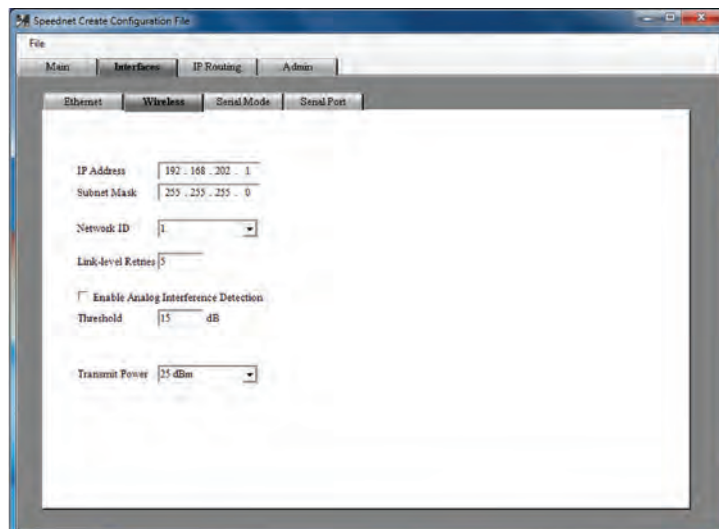


Figure 40. Network Configuration of the Wireless Interface.

Figure 40 shows the network configuration window for the Wireless Interface. The IP Address, Subnet Mask, Network ID, Link-level Retries, Analog Interference Detection, Threshold, and Transmit Power settings function the same as in the corresponding SpeedNet Client window as described in the “Interfaces Window, Wireless Tab” section starting on page 37. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

Please note that on a given SpeedNet Radio mesh, all the wireless interfaces of the radios should be on the same subnet but should use different individual addresses on that subnet.

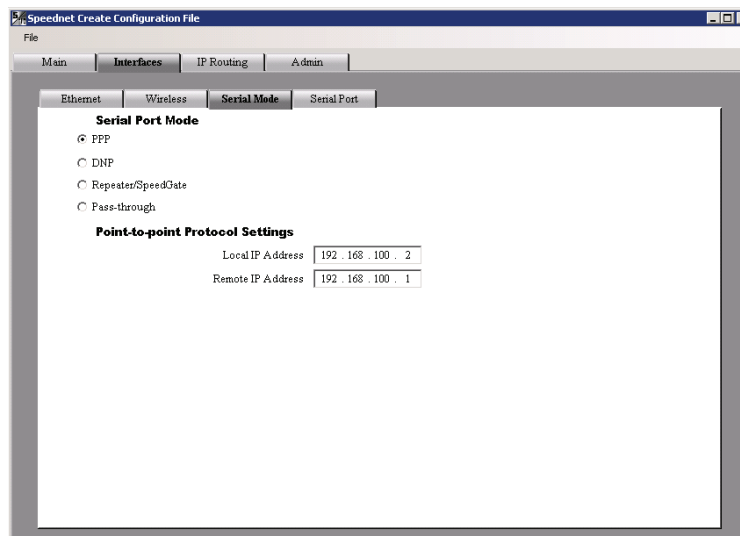


Figure 41. Network Configuration of Serial Port’s PPP Mode Settings.

Four serial port modes are available as described in the “Interfaces Window, Serial Mode Tab” section on page 39.

The Point-to-Point protocol (PPP) provides a standard way to establish a network connection over a serial link. The radio runs PPP over the serial link at a baud rate of 115.2 Kbps, allowing the user to configure the radio in the same way as the standard method over the Ethernet port.

Figure 41 shows the PPP protocol settings. These settings are described in the same “Interfaces Window, Serial Mode Tab” section on page 39. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

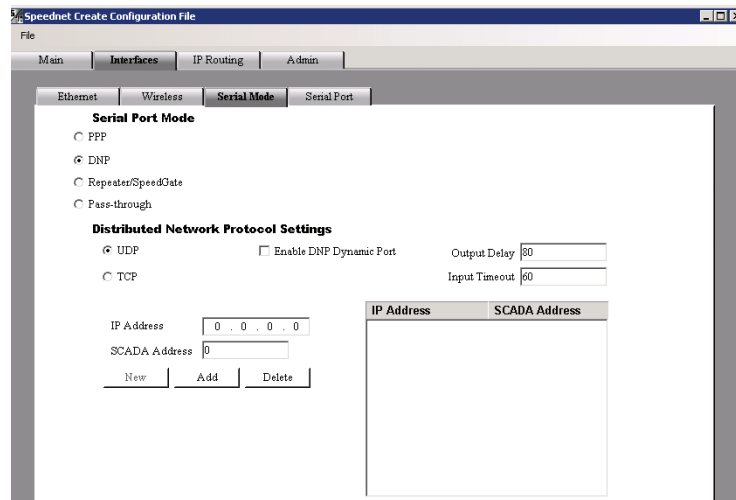


Figure 42. Network Configuration of Serial Port’s DNP Mode Settings.

Figure 42 shows network configuration of the distributed network protocol settings. These settings correspond to those in the SpeedNet Client Tool described in the “DNP Serial Mode” section on page 40. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

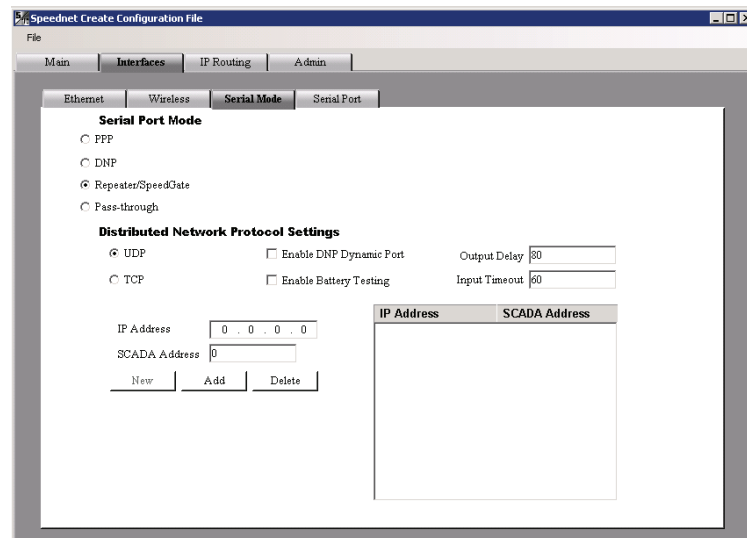


Figure 43. Network Configuration of Serial Port’s Repeater SpeedGate Mode Settings.

Figure 43 shows the Repeater/SpeedGate Mode settings. For this mode, the serial port operates at a baud rate of 38.4k baud, 8-bit data, no parity, and 1-stop bit. The settings in this dialog correspond to those in the SpeedNet Client Tool described in the “Repeater/SpeedGate Serial Mode” section on page 41. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

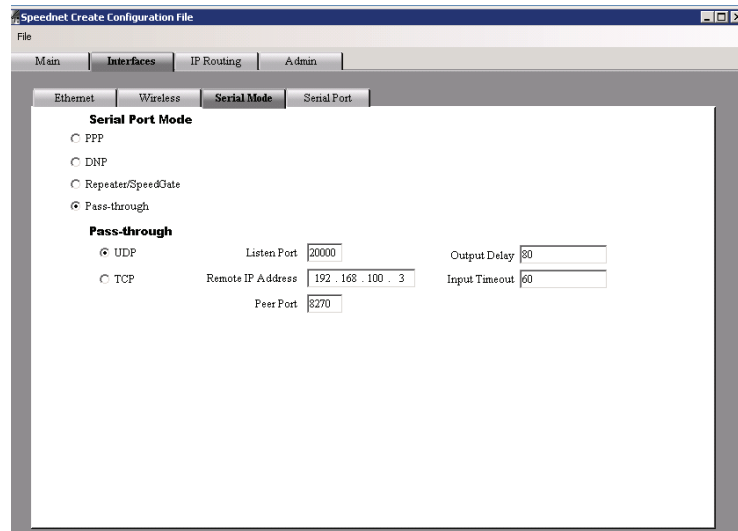


Figure 44. Network Configuration of Serial Pass-Through Mode Settings.

Figure 44 shows the Pass-through settings. The settings in this dialog correspond to those in the SpeedNet Client Tool described in the “Serial Pass-through Mode” section on page 43. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

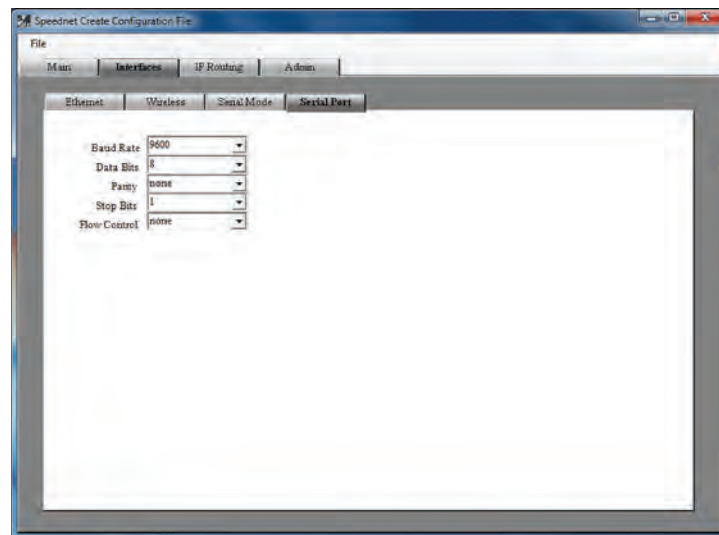


Figure 45. Network Configuration of Serial Port's Settings.

Figure 45 shows the Serial Port settings. These settings correspond to those in the SpeedNet Client Tool described in the “Interfaces Window, Serial Port Tab” section on page 42. There is no **Apply** button on this window because application to a radio is deferred until uploaded using the SpeedNet Client tool.

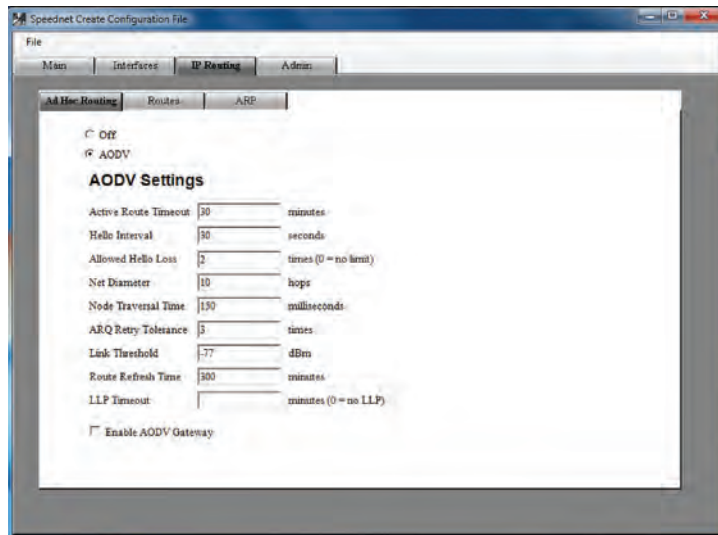


Figure 46. Network Configuration of AODV Settings.

Figure 46 shows configuration of the AODV Settings. These settings correspond to those in the SpeedNet Client Tool described in the “IP Routing Window, Ad Hoc Routing Tab” section on page 44. There is no **Apply** button on this window since application to a radio is deferred until uploaded using the SpeedNet Client tool.

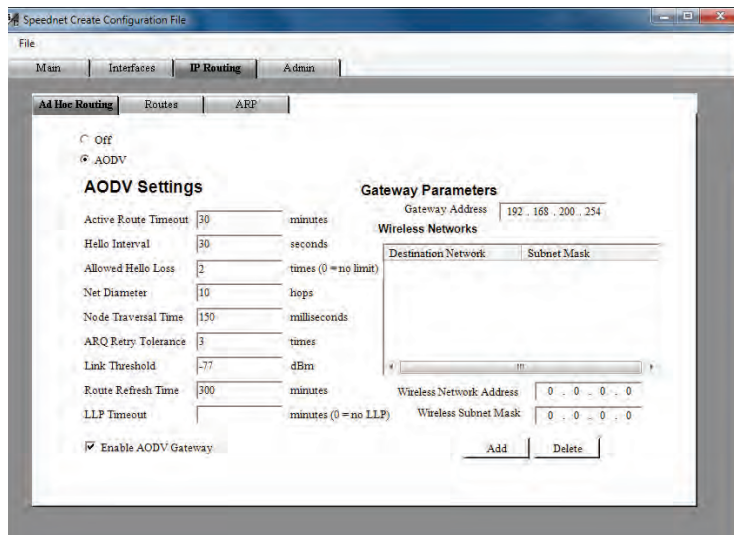


Figure 47. Network Configuration of the AODV Gateway Function

Figure 47 shows configuration of the AODV Gateway Parameters. These settings correspond to those in the **AODV Gateway Settings** screen shown in Figure 72 on page 47. It is important to note that only one AODV Gateway should be active in a SpeedNet mesh at any given time.

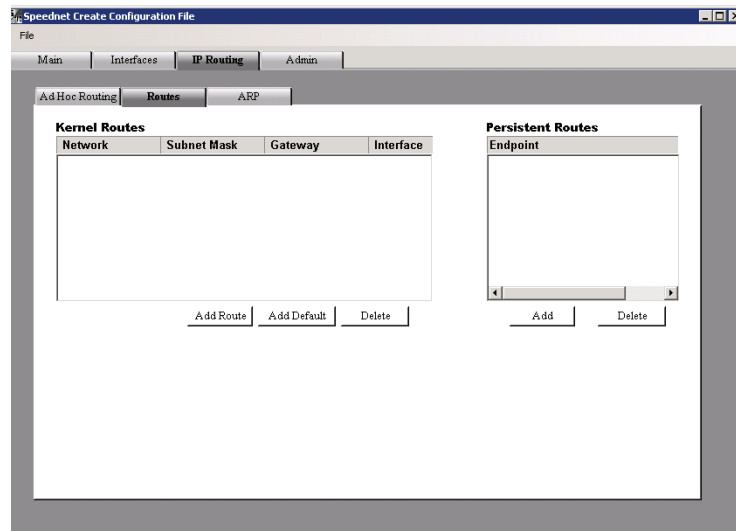


Figure 48. Network Configuration of Routes.

Figure 48 shows network configuration of routes. These settings correspond to those in the SpeedNet Client Tool described in the “IP Routing Window, Routes Tab” section on page 48.

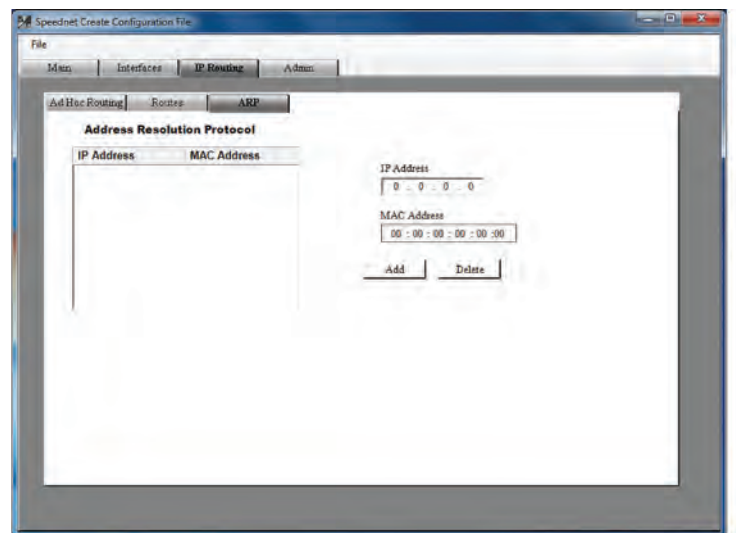


Figure 49. Network Configuration of Address Resolution Protocol.

Figure 49 shows the network configuration of Address Resolution Protocol (ARP). These settings correspond to those in the SpeedNet Client Tool described in the “IP Routing Window, ARP Tab” section on page 49.

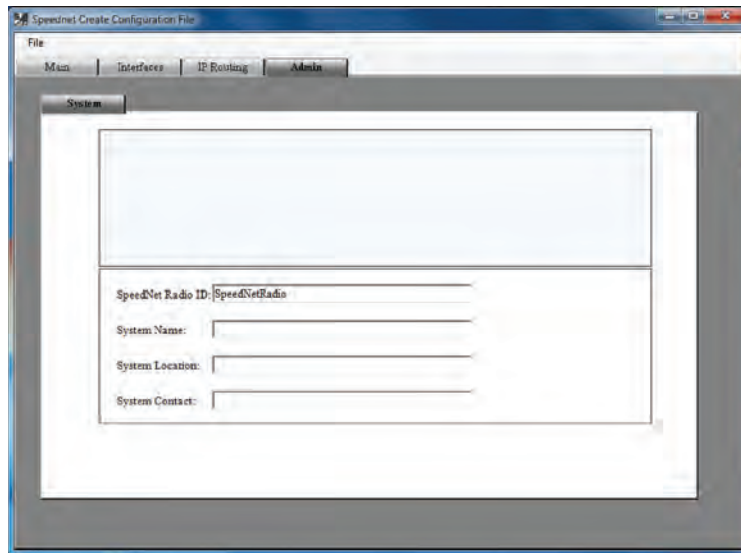


Figure 50. Network Configuration of System Information.

Figure 50 shows the network configuration of System information. These settings correspond to those in the SpeedNet Client Tool in the “Admin Window, System Tab” section on page 53.

Key Updater Tool

The Key Updater tool is a PC-based utility that provides ease of use in updating encryption keys remotely for a group of radios. The Key Updater tool reads a text file containing radio IP addresses and updates the radio encryption keys in sequence.

The Key Updater tool is supported from SpeedNet Radio Firmware Version 2.5.3 onwards.

STEP 30. Launch the Key Updater application. The main window will open. See Figure 51.



Figure 51. Key Updater application launch window.

Step 31

STEP 31. Open a valid SAD file. Once you choose an SAD file, enter the username and password for that SAD file, and click the **OK** button. See Figure 52.

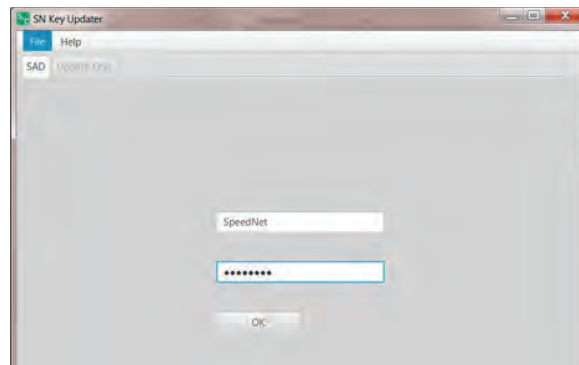


Figure 52. SAD dialog box

STEP 32. Create a text file with the wireless address list of radios whose security file we want to change.

STEP 33. Select the Keyset and click on the **Update Keys** tab. See Figure 53.

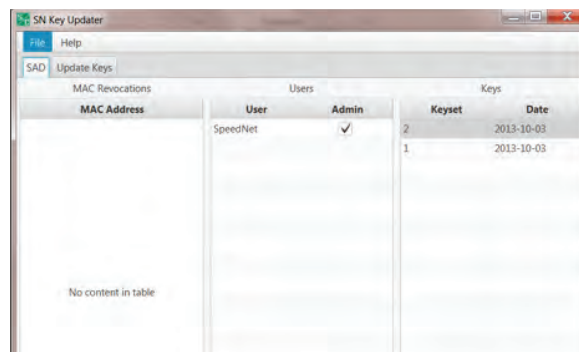


Figure 53. Update Keys dialog box.

STEP 34. Enter username and password. See Figure 54.

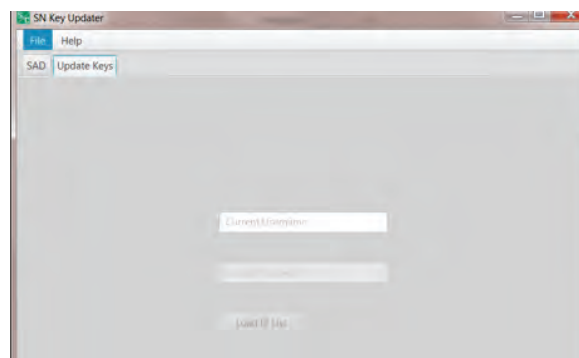


Figure 54. Username and Password dialog box.

STEP 35. Click on the **Load IP List** button, then choose text file. Click the **OK** button.

STEP 36. Choose a timeout value—it's the amount of time the Key Updater application waits for the process to complete for a single radio before timing out. See Figure 55.

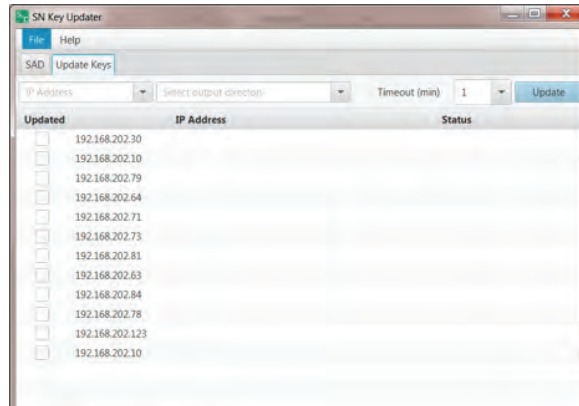


Figure 55. Key Updater IP address listing and Timeout selection window.

STEP 37. Choose an output folder. See Figure 56.

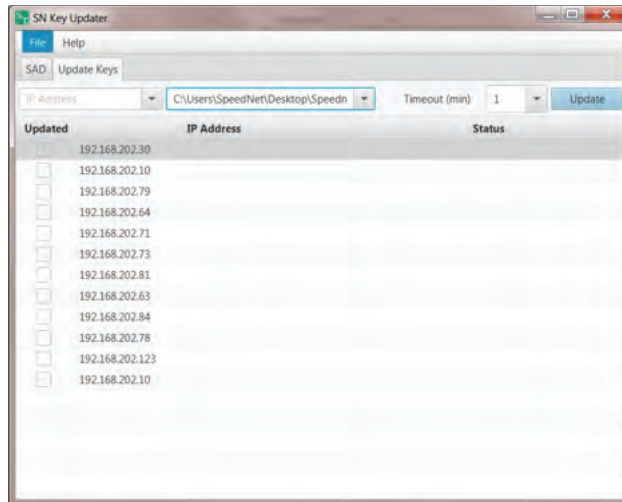


Figure 56. Key Updater IP address listing and Output folder selection window.

STEP 38. Choose an output folder. See Figure 57.

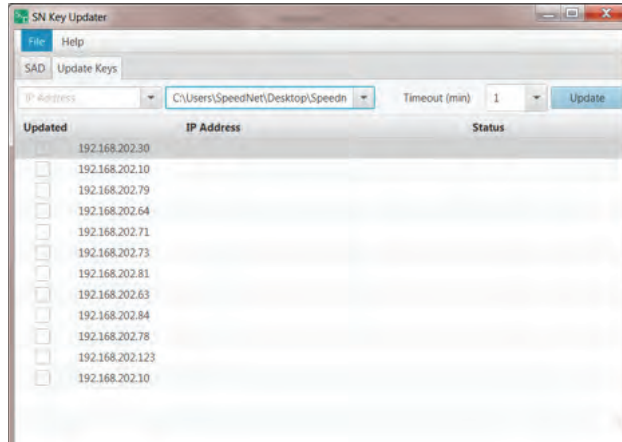


Figure 57. Key Updater IP address listing and Output folder selection window.

STEP 39. Click **Update** button. Choose LAN interface of Head End Radio. See Figure 58.

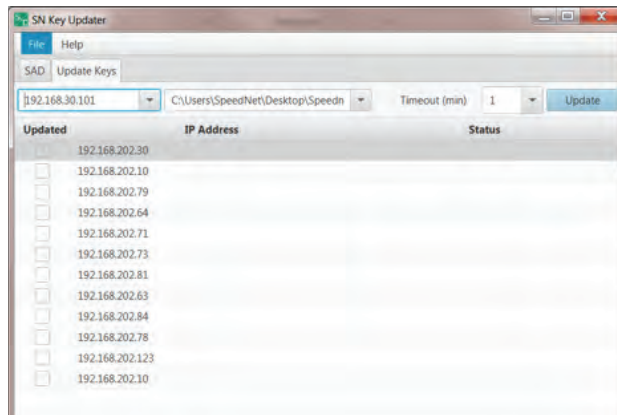


Fig 58. Key Updater IP address listing window.

STEP 40. A checkmark next to the IP address indicates the radio is successfully updated. In case of failures, click the Update button again after the update has been attempted for all radios and the **Update** button is highlighted. See Figure 59.

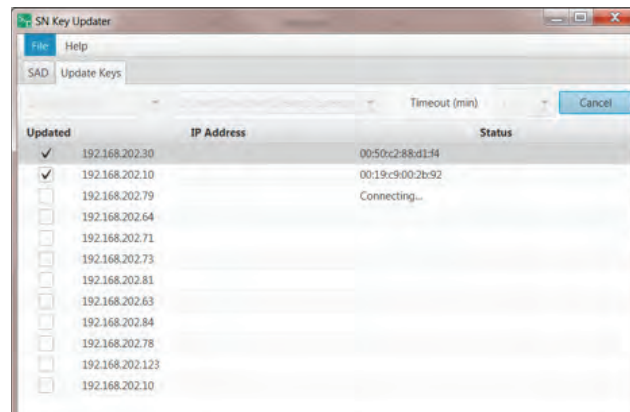


Figure 59. Key Update status.

Overview

The configuration and management of a SpeedNet Radio network is achieved using the SpeedNet Radio Client Tool application and the IntelliTeam® CNMS Communication Network Management System tool. The Client Tool, based on the Simple Network Management Protocol (SNMP), provides a secure method for viewing or modifying SpeedNet Radio configuration parameters. The Client Tool can also update SpeedNet Radio firmware.

Logging In

Launch the SpeedNet Client Tool, and the **Login** dialog box will open. In the IP Address field, enter the IP address of the SpeedNet Radio's Ethernet interface; the default is 192.168.200.1. When the radio mesh has been configured, you can also log in using the wireless IP address.

When logging in to a SpeedNet Radio for the first time after a factory reset, the user name will be "initial" and the factory password will be the radio's unique MAC address listed as MAC ID on the radio label. The MAC address must be entered with all lowercase characters and without any separators (for example: 00c919eea1b2). The **Login** window and label are shown in Figures 60 and 61. As shipped from S&C, SpeedNet Radios are configured using a standard SAD file that includes a default username and password. Contact S&C to obtain these credentials.

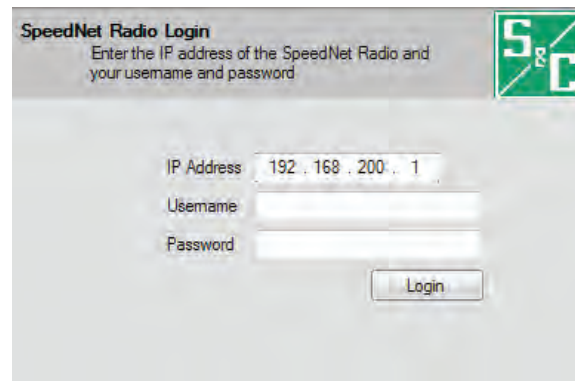


Figure 60. The SpeedNet Login dialog box.



Figure 61. Location of the SpeedNet Radio MAC Address label.

After entering the appropriate log-in information, click the **Login** button to connect to the SpeedNet Radio. The **Main** window will be displayed. See Figure 60.

Main Window



Figure 62. SpeedNet Client Main window.

The **Login** button submitted the username and password supplied to the radio specified by the IP address and causes the client tool to fetch the configuration information from the radio. Further transactions through the client tool tabs use this same information (IP address, username, and password) to get and set data in the radio. Note that logging in from the client tool does not produce a persistent session or state change in the specified radio. Further, logging in from one client tool does not preclude logging in from other client tools on other PCs, provided they also have the valid log-in information (IP address, username, and password). See Figure 60 on page 33.

A description of the various fields and tabs is provided below:

- The display in the upper-right corner of the **Main** window shows the Location, the Radio ID (node name), Radio IP address, Radio Status, and user's security access level. See Figure 60 on page 33
- **SNMP Timeout**—The SNMP protocol automatically resends control data after a period of time. The SNMP Timeout control is used to adjust the timeout value. In the case of a busy network or when traversing many wireless hops, you may wish to increase the SNMP timeout. The default value will work in most situations
- **Connect To**—The **Connect To...** button allows you to connect to a different SpeedNet Radio by opening the SpeedNet Radio Login window

Other configuration functions are accessed by clicking on the appropriate tabs, as follows:

- **Interfaces**—The Interfaces window is used to configure the Ethernet, wireless, and serial interfaces
- **IP Routing**—The IP Routing window is used to configure the routing settings for the wireless network, including the use of mesh networking or static routes
- **Security**—The Security window is used to configure wireless network encryption and view the MAC Address Revocation list
- **Admin**—The Admin window is used to assign the Radio ID (radio node name), upload security and network configuration files, reboot the radio, and install new radio firmware
- **Statistics**—This window provides detailed information regarding radio performance

NOTICE

A login from the SpeedNet Client Tool is somewhat different from other logins, such as telnet or remote desktop sessions. The communication between the client tool and the radio is fundamentally transactional. When the user logs in using the SpeedNet Client Tool, the client tool contacts the radio via SNMPv3/UDP/IP using the username and password credentials provided, and attempts to fetch the radio's configuration information. If the credentials are incorrect, the client tool informs the user that the login failed. If the credentials are correct, the client tool displays basic configuration information just fetched in the upper right corner of the Main window, and shows the Status as connected. Each subsequent transaction, until the client tool is directed to a new radio, is individually authenticated via SNMPv3 using the credentials provided by the user at the start of the session and stored in the client tool. No state of the SpeedNet Client Tool session is stored in the radio, and the client tool does not poll the radio to update displayed information between user transactions. Thus, the radio can have several client tools from different PCs logged in at the same time. Also, the radio can undergo changes such as a reboot behind the client tool session with no impact on the client tool, except that transaction attempts (e.g. changing to another client tool tab or clicking an **Apply** button) during the reboot will not function.

Interfaces Window, Ethernet Tab

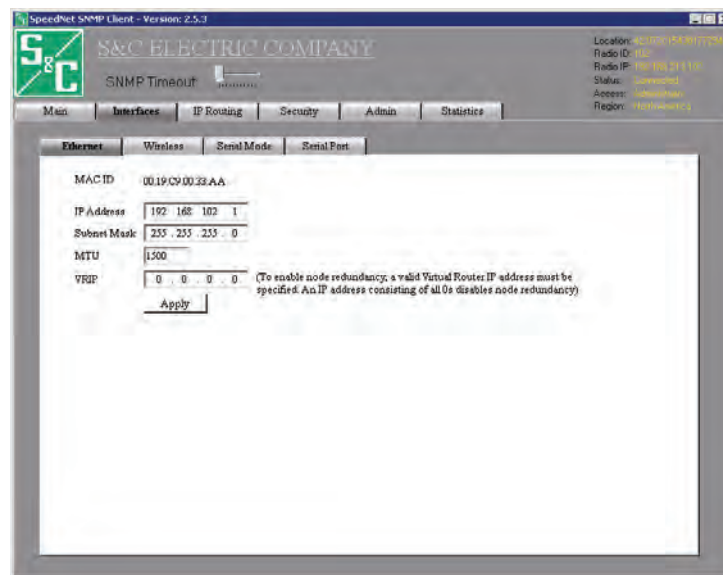


Figure 63. Configuration of the Ethernet interface.

Figure 63 shows the **Ethernet Interface** configuration window. On a given SpeedNet Radio mesh, the configurations of all the Ethernet interfaces should differ so there is no overlap between the Ethernet port subnets or between the Ethernet port subnets and the wireless subnet.

Redundancy for SpeedNet Head-End Radios and SpeedNet Gateways is supported using the Ethernet interface (and not the Wireless interface). This redundancy feature provides fault tolerance to head-end radios (with the **AODV Gateway** mode on or off), and only applies to non-serial configurations. Because a single head-end radio is a single-point of impairment, redundancy improves communication reliability. This is important for head-end radios because they are the link to the customer enterprise network.

Redundancy is enabled by provisioning a virtual IP address for a pair or grouping of radios on their Ethernet interface. The radio pair is addressed by its virtual IP address; they will negotiate and communicate over their wired Ethernet subnet and form a master/standby group.

The Ethernet addresses of the redundant nodes are different, but they should be configured on the same subnet, communicating via a switch. The head-end radios will negotiate and communicate over their wired Ethernet subnet and form a master/standby group. The head-end radio with the higher value in its last octet will be the master. If the virtual address is accidentally set to the same as the Ethernet IP address, redundancy will not be enabled.

When enabling redundancy, only /24 and higher LAN addresses on the Ethernet port should be allowed so the last octet of the Ethernet IP addresses are unique on the LAN.

When using a redundant configuration, Ethernet multicast must be enabled on the subnet.

The Wireless IP addresses of the redundant nodes should be configured to be different.

The standby radio takes itself off the air and disables its RF interface.

Each member of a redundant set of SpeedNet radios must have its own antenna. The Interfaces window provides tabs that can be used to configure each interface of the SpeedNet Radio. The tab will provide a list of configurable options for the selected interface.

The Ethernet tab, shown in Figure 63 on page 35 is used to configure the SpeedNet Radio's Ethernet interface. The following parameters can be configured:

- **MAC ID**—This read-only field displays the unique Media Access Control (MAC) address of the SpeedNet Radio. No two network devices will use the same MAC address
- **IP Address**—Specifies the IP address of the Ethernet interface of the SpeedNet Radio. The default IP Address is 192.168.200..
- **Subnet Mask**—Specifies the subnet mask of the Ethernet interface. The default subnet mask is 255.255.255.0
- **MTU**—The Maximum Transmit Unit (MTU) specifies the maximum Ethernet packet size (in bytes) that can be transmitted without being fragmented. The default value of 1500 bytes should be appropriate for most applications
- **VRIP**—The VRIP parameter provides a means to configure redundancy for head-end radios/AODV Gateways. Both the redundant nodes are recommended to be physically co-located and must be configured with the same VRIP. Setting a value of 0.0.0.0 for the VRIP disables redundancy
- **Apply**—Saves changes made to the configuration of the **Ethernet** tab. Changes will not be saved if you change to a different configuration tab without first clicking the **Apply** button

Note: Redundancy is not supported on the SpeedNet ME, so the VRIP field is not available

Interfaces Window, Wireless Tab

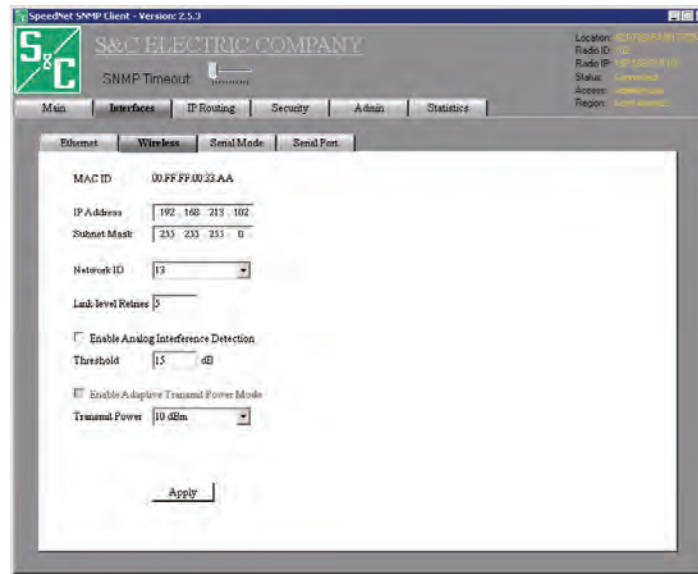


Figure 64. The Wireless interface configuration window.

The **Wireless** tab, shown in Figure 64, is used to configure the SpeedNet Radio wireless interface. Note that several features are for reference only and will appear grayed out in the client tool. Some of the following parameters can be configured:

- **MAC ID**—This read-only field displays the unique Media Access Control (MAC) address of the SpeedNet Radio wireless interface. The wireless MAC ID is based on the Ethernet interface MAC ID but with the second and third sets of digits replaced with “FF”
- **IP Address**—Specifies the IP address of the wireless interface of the SpeedNet Radio. The default IP address is 192.168.202.1. This address must be unique for each radio on the wireless network
- **Subnet Mask**—Specifies the subnet mask of the wireless interface. The default subnet mask is 255.255.255.0
- **Network ID**—Specifies the frequency-hopping pattern that will be used by the SpeedNet Radio. To communicate with each other, SpeedNet Radios in the same wireless network must use the same network ID setting. Note that SpeedNet networks can be located close to each other with minimal network interference by configuring a separate network ID for each network. The network ID parameter has a value range of 1-16, with a default value of 1

- **Link-level Retries**—Specifies the number of retries this radio should send when a positive acknowledgement has not been received for a packet. Setting this parameter too low will cause packets to be dropped unnecessarily in the presence of temporary interference or other errors. Setting this parameter too high could cause flooding of retries on the radio mesh when none will succeed, for example if the intended receiver's antenna breaks. The recommended value is 5
- **Enable Analog Interference Detection**—This feature detects analog radio interference with the 902-928-MHz frequency band, allowing the SpeedNet Radio to temporarily avoid transmitting on frequency channels that have interference levels above the average received in those channels
- **Threshold**—This parameter determines the number of dB above the average signal in a particular frequency channel that will cause Analog Interference Detection to start functioning to skip that channel in the hopping sequence. The default value is 15 dB.
- **Enable Adaptive Transmit Power Mode**—(Reference only) This feature causes the SpeedNet Radio to adjust the output power level to the minimum level required to achieve a solid link. The output power level will vary between each radio link. When this feature is enabled, the Transmit Power parameter will be replaced with “min” and “max.” These options are used to determine the minimum and maximum output power levels to be used when **Adaptive Transmit Power** mode is enabled
- **Transmit Power**—This setting determines the maximum output power level to be used for wireless transmissions by the SpeedNet Radio. Options are: 10 dBm, 20 dBm, 25 dBm, and 30 dBm. The default value is 30 dBm
- **Apply**—Saves changes made to the wireless configuration. Changes will not be saved if you change to a different configuration tab without first clicking the **Apply** button

Interfaces Window, Serial Mode Tab

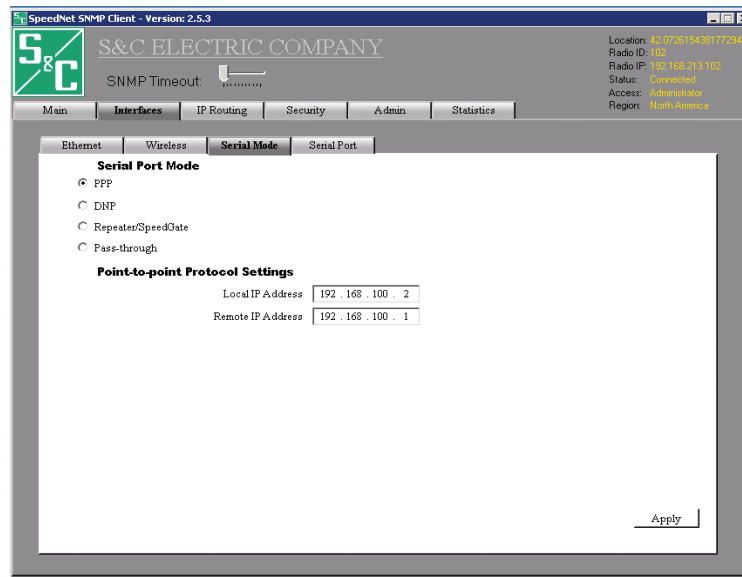


Figure 65. The Serial Mode interface configuration window.

The following serial port modes are available: See Figure 65.

- **PPP**—The Point-to-Point Protocol (PPP) mode is used for emulating an Ethernet connection over a serial interface. This is currently used for communication with a SpeedNet Radio in an IntelliRupter fault interrupter through the fault interrupter's Wi-Fi interface. SpeedNet Radios do not route traffic to other radios from the PPP interface due to security concerns
- **DNP**—The Distributed Network Protocol (DNP) mode is used for transferring DNP data between the SpeedNet Radio serial port and other Ethernet devices
- **Repeater/SpeedGate**—The Repeater/SpeedGate mode is used for SpeedNet Radios that operate as fixed repeaters within a network
- **Serial Pass-Through**—The Serial Pass-Through feature allows support for legacy equipment on the serial port using non-DNP3 serial protocols, such as Modbus
- **Apply**—Saves changes made to the **Serial Mode** window. Changes will not be saved if you select a different configuration tab without first clicking the **Apply** button

PPP Serial Mode

The following options are available when PPP is the selected serial port mode, as shown in Figure 65.

- **Local IP Address**—IP address (Ethernet Interface) assigned to the SpeedNet Radio's end of the PPP link
- **Remote IP Address**—IP address assigned to the remote device of the PPP link

Point-to-point Protocol Settings	
Local IP Address	192 . 168 . 100 . 2
Remote IP Address	192 . 168 . 100 . 1

Figure 66. PPP Protocol settings.

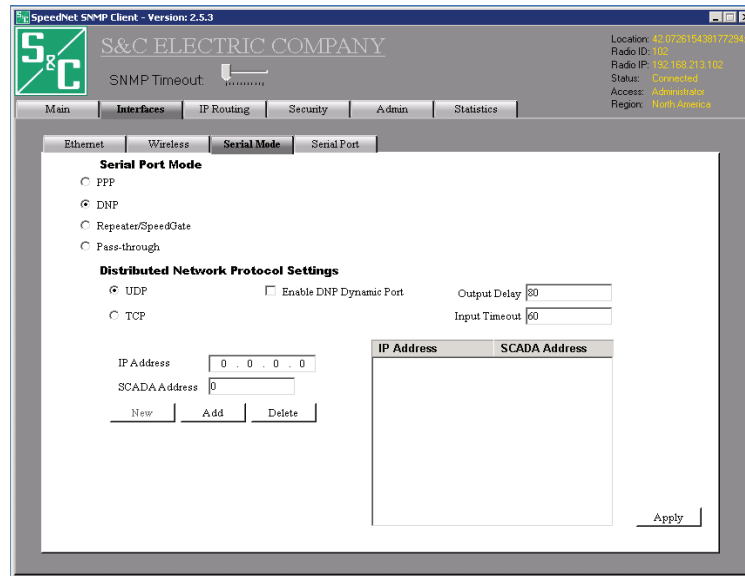


Figure 67. Distributed Network Protocol settings.

DNP Serial Mode

The following options are available when DNP is the selected serial port mode, as shown in Figure 67.

- **UDP/TCP**—Determines which transport control protocol, TCP or UDP, will be used for DNP communication. UDP is the default setting
- **Enable DNP Dynamic Port**—Enabling the DNP Dynamic Port feature causes the SpeedNet Radio to monitor SCADA traffic to determine the source port for each data stream. Port information is stored internally, allowing the SpeedNet Radio to know which port to send received packets to on the SCADA master. While many SCADA masters use port 20,000 for SCADA communications, some of them use a different port for each device
- **IP Address**—When creating a DNP table entry, this value is the IP Address
- **SCADA Address**—When creating a DNP table entry, this value is the SCADA address. The valid range of SCADA addresses is 0-65536
- **Add**—After entering an IP address and the corresponding SCADA address, click the **Add** button to add the entry to the DNP table
- **Delete**—To delete an entry from the DNP table, select the entry in the table and click the **Delete** button
- **Output Delay**—This value defines the amount of time (in milliseconds) between transmitting DNP packets to the SpeedNet Radio's serial interface after they are received over the wireless interface. This feature has been added to accommodate legacy equipment that cannot receive back-to-back data packets as quickly as a SpeedNet Radio can deliver them. The default value is 80 milliseconds
- **Input Timeout**—This value defines the amount of time (in milliseconds) that the serial interface will wait before sending a packet after data is received. The default value is 60 milliseconds

Multiple SCADA Masters

SpeedNet Radios have a feature that allows multiple SCADA masters that use the same SCADA address to connect to a single SpeedNet Radio. When this feature is enabled, the connected SpeedNet Radio continually monitors DNP traffic. For multiple SCADA masters using the same SCADA address, the SpeedNet Radio will consider the master to be the device that sent the most recent data packet. If the active SCADA master experiences a failure, the SpeedNet Radio will automatically forward packets from the backup SCADA master.

Configuring this feature is simple. When building the SCADA table using the UDP/IP transport option, each SCADA master is assigned the same SCADA Address, and each SCADA master has a unique IP address.

For example, assume there are two SCADA master devices, one with an IP address of 192.168.200.20 (primary SCADA master) and one with an IP address of 192.168.200.30 (secondary SCADA master). To create the table entry for the primary SCADA master, enter 192.168.200.20 into the IP Address field. Enter 25 into the SCADA address field. To create the table entry for the secondary SCADA master, enter 192.168.200.30 into the IP Address field. Enter 25 into the SCADA address field.

Repeater/SpeedGate Serial Mode

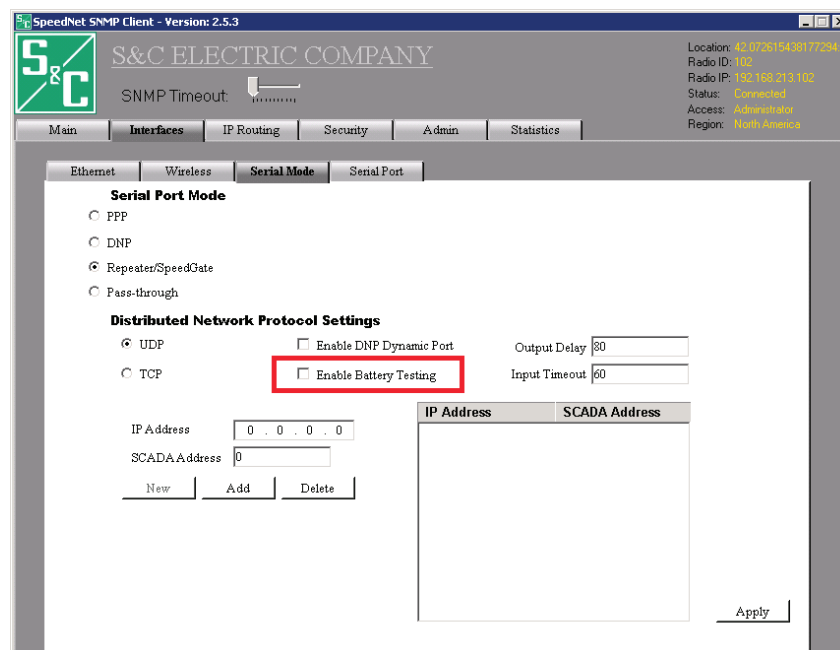


Figure 68. Repeater SpeedGate settings.

The SpeedNet Repeater/SpeedGate **Serial Port** mode provides the same configuration parameters as the DNP **Serial Port** mode, see Figure 68 for details. As shown in Figure 68, one additional parameter is available when the Repeater/SpeedGate **Serial Port** mode has been selected.

- **Enable Battery Testing**—Provides the ability for SpeedNet Radios to periodically test the status of the connected backup battery system in S&C SpeedNet repeaters and SpeedGate systems. This feature multiplexes proprietary battery charger control and status messages into the serial port stream that is also used for DNP. The charger provides another serial connection for DNP communication to other devices that have the battery charger messages stripped out. When this feature is enabled, the results of battery tests can be seen on the **Batt Status** tab of the **Statistics** window. See Figure 88 on page 60. When **Enable Battery Testing** is configured, within 90 seconds the first battery test will occur. When this test has completed, the battery will be tested automatically every 24 hours.

If the Repeater/SpeedGate loses ac control power, the battery test will run once an hour until ac control power has been restored.

Interfaces Window, Serial Port Tab

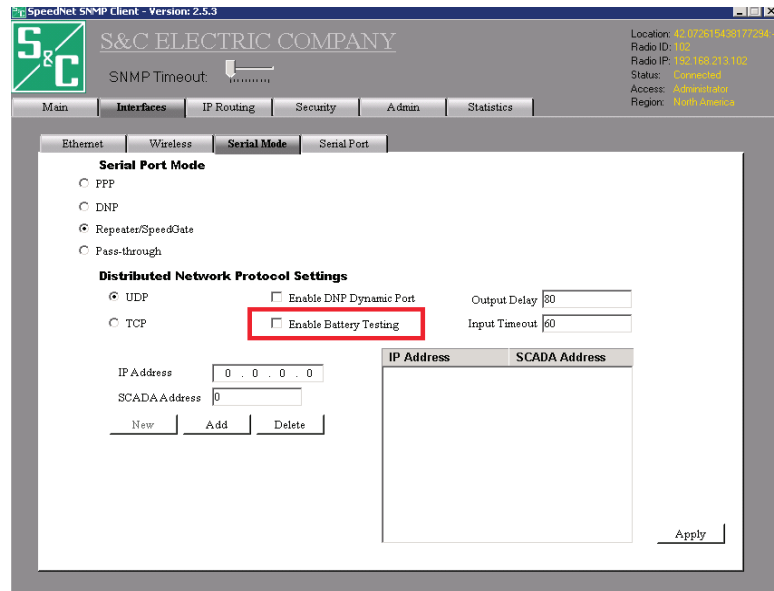


Figure 69. Serial Port interface configuration window.

The **Serial Port** tab is only available when **DNP** is selected as the serial port mode. As shown in Figure 69, the **Serial Port** tab is used to configure the communication parameters for the SpeedNet Radio's serial port. The following parameters can be configured:

- **Baud Rate**—Determines the bit rate used for serial communications; the default value is 9600
- **Data Bits**—Determines the number of data bits within each character; the default value is 8
- **Parity**—Determines the setting for the parity bit within each character; the default value is none
- **Stop Bits**—Determines the number of stop bits that follow each character; the default value is 1
- **Flow Control**—Configures the type of flow control that is used for serial data communication; the default value is none

Serial Pass-Through

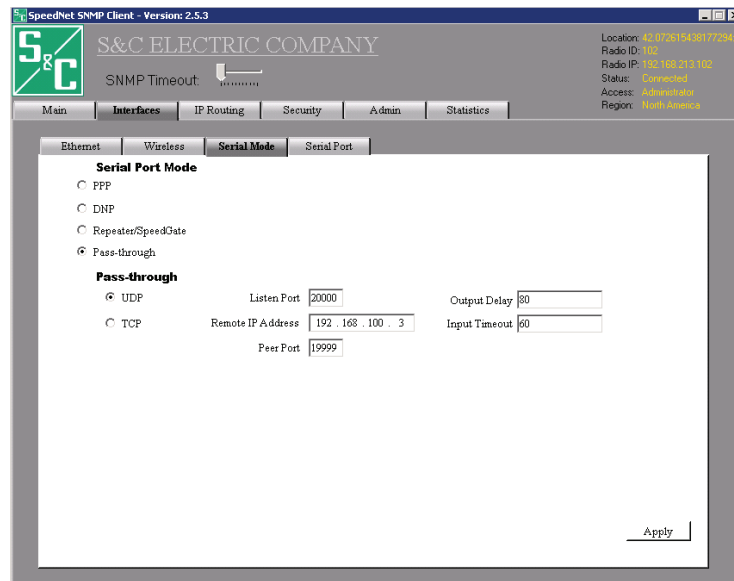


Figure 70. Serial Pass-Through configuration window.

The **Serial Pass-through** feature allows support for legacy equipment on the serial port using non-DNP3 serial protocols, such as Modbus.

The following options are available when **DNP** is the selected serial port mode, as shown in Figure 70.

- **UDP/TCP**—Determines which transport control protocol—TCP or UDP—will be used for pass-through communication; UDP is the default setting
- **Listen Port**—The IP port the radio listens on for incoming messages
- **Remote IP Address**—The IP address assigned to the remote device of the pass-through link
- **Peer Port**—The Remote IP port the radio sends the serial message to
- **Output Delay**—The value that defines the amount of time (in milliseconds) between transmitting serial packets to the SpeedNet Radio's serial interface after they are received over the wireless interface (This feature has been added to accommodate legacy equipment that cannot receive back-to-back data packets as quickly as a SpeedNet Radio can deliver them. The default value is 80 milliseconds.)
- **Input Timeout**—The value that defines the amount of time (in milliseconds) the serial interface will wait before sending a packet after data is received; the default value is 60 milliseconds

Persistent Routes

The **Persistent Routes** feature will establish a route to a specific destination before any application traffic is initiated. The **Persistent Routes** feature runs with AODV enabled and implements a keep-alive mechanism between a source and a destination.

The **Persistent Routes** feature is useful when traffic must keep flowing to specific paths in the network. It will also reduce delay and improve reliability between the nodes configured with the **Persistent Routes** feature.

It is important to note that entries for persistent routes only need to be configured in each end-point radio. No intermediate hops need to be entered. The AODV Mesh will automatically determine the route.

The following options are available:

- **Add**—The **Add** button is used to add persistent routes to the route table. Click the **Add** button, enter the Endpoint's IP address, and click the **OK** button to add a persistent route
- **Delete**—To delete a route from the route table, select the route, then click the **Delete** button to remove the route from the route table

IP Routing Window, Ad Hoc Routing Tab

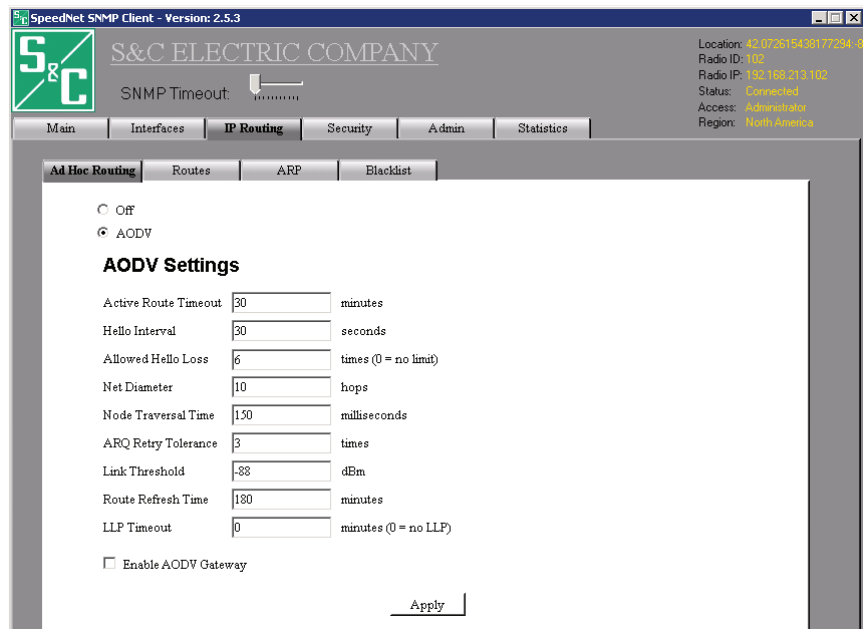


Figure 71. The Ad Hoc Routing IP configuration window.

The **IP Routing** window provides a list of tabs that can be used to configure the routing performance of a SpeedNet Radio. Selecting a tab will provide a list of configurable options.

The **Ad Hoc Routing** tab, shown in Figure 71, is used to enable, disable, or configure the embedded ad hoc (mesh) routing protocol. The embedded ad hoc routing protocol is a customized version of Ad-hoc On-demand Distance Vector (AODV). The following parameters can be configured:

- **Off**—Selecting **Off** will disable the automated mesh networking protocol. When disabled, static routes must be entered manually on the **Routes** tab for all endpoints this radio needs to reach. No combination of automatic AODV routing and static routing is supported
- **AODV**—Selecting **AODV** will enable the embedded mesh networking protocol allowing network routes to be created and maintained automatically to the best next hop neighbor from the SpeedNet Radio. All radios in the network must enable AODV to use the feature. Selecting **AODV** is recommended for ease of configuration, robustness to radios going down, and ease of adding radios to the mesh. The remaining configuration options on the **Ad Hoc Routing** tab pertain specifically to the mesh networking protocol
- **Active Route Timeout**—The **Active Route Timeout** parameter determines how long a SpeedNet Radio should wait for an inactive data communication route to be removed from the route table. Each time an IP packet is sent over a specific route, a timer begins counting down. If the timer expires before another packet is sent, the route is considered inactive and is removed from the radio's route table. The **Active Route Timeout** value determines the length of this timer. In SCADA polling applications, a timeout value greater than the polling interval is recommended. Note that a route is defined by the IP address of the two endpoints. A given pair of SpeedNet Radios may have several separate routes between them, for example serving different devices on the radios' Ethernet ports. As such, activity on one route between two radios does not preserve other routes between the two radios for traffic with different source/destination IP addresses. The value of this parameter is measured in minutes and the recommended value is 30 minutes

- **Hello Interval**—The **Hello Interval** setting determines how frequently the SpeedNet Radio broadcasts a neighbor beacon message (hello message). Smaller hello interval values increase the wireless network's responsiveness to routing changes but do so at the expense of creating additional network communication overhead. Larger hello interval values decrease the wireless network's responsiveness to routing changes but reduce excessive wireless traffic in the process. This value is measured in seconds and the recommended value is 30 seconds
- **Allowed Hello Loss**—The **Allowed Hello Loss** value determines the number of consecutive hello messages that, when missed, constitutes a link failure that will lead to a new route request for routes incorporating the link that failed. Setting this value too low can cause unnecessary route generation when a hello message is lost because of a temporary circumstance (e.g. a burst of interference or a packet collision). Setting this value too high can cause excessive data loss in a route that is no longer viable because of the persistent failure of a link in the route. The recommended value is 6
- **Net Diameter**—The **Net Diameter** parameter determines the maximum of number of wireless hops between the source and destination nodes, specifically, the maximum number of hops that a route request message can travel. The **Net Diameter** should be set to at least the maximum number of hops expected for application traffic. If the **Net Diameter** is set too low, then route creation may fail because of route requests never reaching the desired endpoint. If the **Net Diameter** is set marginally too low, primary route creation may succeed but creation of a secondary route may not succeed in the case of a link failure along the primary route. If the **Net Diameter** is set too high, route requests may propagate needlessly to too many radios, generating excessive overhead. Setting the **Net Diameter** too high is a more critical issue in high-density connected mesh deployments than in linear deployments. In mesh deployments, the overhead incurred by the **Net Diameter** can increase as the square of the diameter. Do not set this value to the number of radios in the mesh. Set it to the lowest possible value that allows for redundancy. The recommended value is 10 hops
- **Node Traversal Time**—The **Node Traversal Time** value provides an estimate of the time required for a packet to traverse one wireless hop. This value affects how long a SpeedNet Radio waits before resending a route request packet. This value is measured in milliseconds and the recommended value is 150 msec
- **ARQ Retry Tolerance**—The **ARQ Retry Tolerance** parameter allows a configurable number of successive, unique packet delivery retries prior to terminating a route. When this number of successive retries is reached, a radio node is able to know more quickly that its next hop radio neighbor is no longer available to route packets, and a route will be built around that unavailable neighbor if there is another valid neighbor.

This configuration parameter is useful to balance the identification of an unavailable neighbor with packet delivery success rates so more expedient routing may be performed around an unavailable node. The recommended value is 3

- **Link Threshold**—SpeedNet Radio only considers a neighboring radio node valid, if its signal strength is above a configured threshold, called the grayzone threshold

A radio neighbor with signal strength above the grayzone threshold is considered viable to build routes through, and a neighbor below this threshold will not be used for routing from that specific radio

The grayzone threshold removes excessive neighbors from a SpeedNet network. The recommended number of neighbors is between 2 and 25. If more than 25 neighbors are visible, setting the grayzone threshold to a stronger signal strength value reduces the number of neighbors and their routing protocol maintenance traffic. Excessive neighbors can lead to network congestion. The grayzone threshold configuration parameter name is **Link Threshold**.

- **Route Refresh Time**—Once a route has been established, periodic route updates are broadcast to the wireless network. The **Route Refresh Time** determines how frequently route update messages are broadcast. If the **Route Refresh Time** is too short, there may be excessive overhead on the radio network in carrying the route updates. If the **Route Refresh Time** is too long, the network may be slow to optimize routes when better routes become available (e.g. when a new repeater is added or when temporary interference abates). The recommended value is 180 minutes
- **LLP Timeout**—SpeedNet normally attempts to find the path between nodes that has the fewest number of hops. However, sometimes the shortest path is not always the optimal one because of conditions such as RF interference, line-of-sight impediments, multipath propagation, and network congestion. If **Local Link Preference** mode is enabled and a radio experiences an inability to deliver messages through a given neighboring node, SpeedNet will attempt to avoid that neighbor if alternate neighbors are available to deliver the messages

LLP can co-exist with the Blacklisting feature introduced in SpeedNet Revision 2.4.7. Radios can be added to the blacklist and not used for routes. With LLP on, these neighbors won't be used, and LLP will search for alternate routes if the radio is unable to deliver messages through a neighboring mode

The **LLP Timeout** parameter specifies when a neighbor who had been put in the LLP blacklist is made available as a routing option. Setting **LLP Timeout** to 0 effectively disables LLP. When LLP is enabled, the recommended value for **LLP Timeout** is 1440 minutes (1 day)

- **Apply**—Saves changes made to the configuration of the **Ad Hoc Routing** tab. Changes will not be saved if you change to a different configuration tab without first clicking the **Apply** button

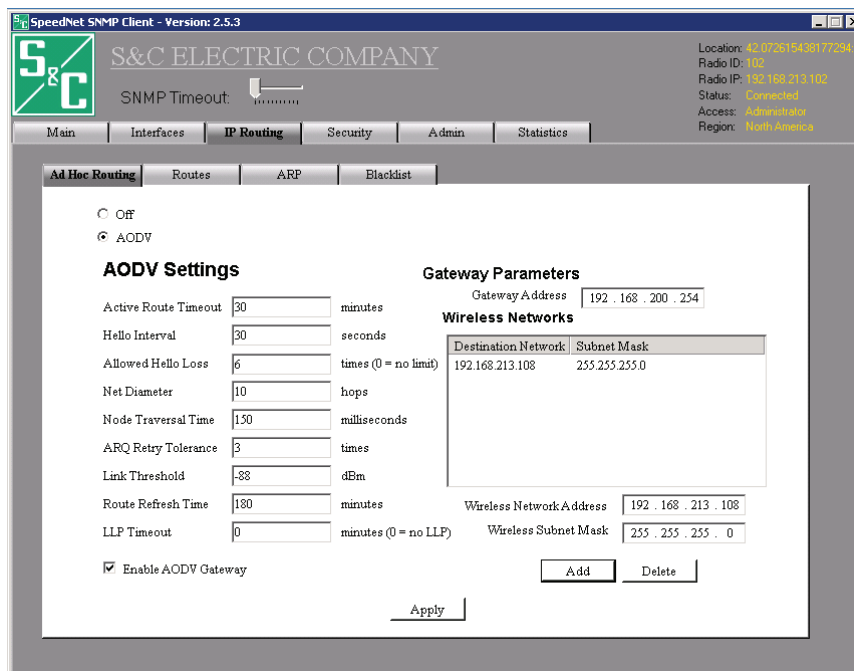


Figure 72. AODV Gateway Settings.

As shown in Figure 72, enabling the **AODV Gateway** feature provides several new configuration options to the **Ad Hoc Routing** tab of the SpeedNet Client tool.

These configuration options are described below: As shown in Figure 72, enabling the **AODV Gateway** feature provides several new configuration options to the **Ad Hoc Routing** tab of the SpeedNet Client tool.

These configuration options are described below:

- **Gateway Address**—The **Gateway Address** is the IP address of the router that the SpeedNet Radio will use as its gateway to the corporate LAN, Internet, or other routable network
- **Wireless Networks**—The **Wireless Networks** table provides a list of wireless networks that are able to use the SpeedNet Radio as a gateway to other networks. The table must be populated to include the Ethernet subnets of all SpeedNet Radios that have a need to use a default gateway to reach devices that are not in the wireless network. This list of networks determines which route requests the AODV Gateway radio should not answer (in other words, what IP traffic the AODV gateway should not attract and forward to the gateway address)
- **Wireless Network Address**—Defines the network(s) for which the SpeedNet gateway radio will act as the gateway. For example, a SpeedNet Radio with an Ethernet IP address of 192.168.200.1 and a subnet mask of 255.255.255.0 would use 192.168.200.0 as the wireless network address portion of the entry
- **Wireless Subnet Mask**—The **Wireless Subnet Mask** works in conjunction with the Wireless Network Address to define the SpeedNet Radios that have a need to use a default gateway
- **Add**—After entering a wireless network address and wireless subnet mask, click the **Add** button to add the wireless network to the table
- **Delete**—To delete a wireless network from the table, select the wireless network from the table and click the **Delete** button

IP Routing Window, Routes Tab

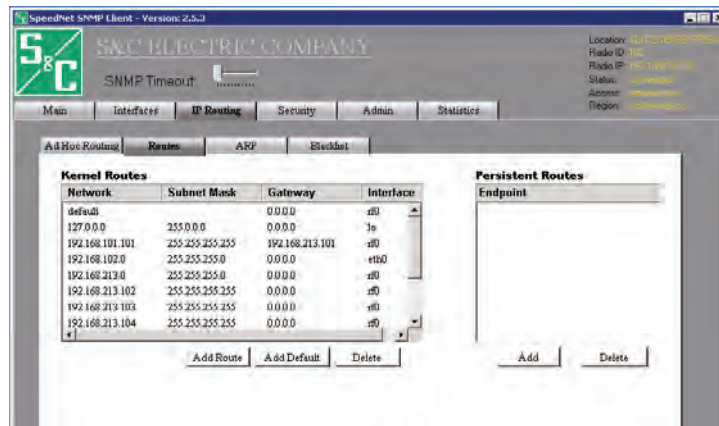


Figure 73. The Routes IP routing configuration window.

The **Routes** tab, shown in Figure 73, is used to view or delete existing data communication route table entries and to add new route table entries for both kernel routes and persistent routes. The following parameters can be configured for kernel routes:

Adding Kernel Routes

- **Route Table**—The **Route Table** displays a list of current routes within the SpeedNet Radio route table. If mesh networking is used, the route table entries will be updated dynamically to reflect changes to the network
- **Add Route**—The **Add Route** button is used to add static routes to the route table and is described in Figure 74
- **Add Default**—The **Add Default** button is used to add a static default gateway to the route table and is described below
- **Delete**—to delete a route from the route table, first select the route. Click the **Delete** button to remove the route from the route table

Adding Static Routes

Clicking the **Add Route** button will add an Add Route section to the **Routing** tab. See Figure 74.

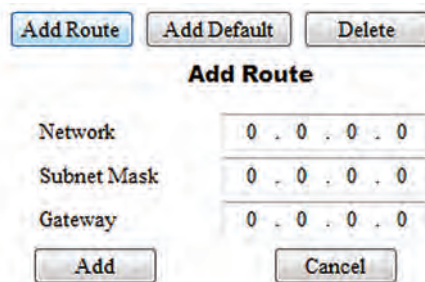


Figure 74. Add Route settings.

The configuration parameters for adding a route are described below:

- **Network**—The destination network for the route that is being created. To enter a static route for a device with an address of 192.168.200.1 and a subnet mask of 255.255.255.0, the network portion of the route entry should be 192.168.200.0
- **Subnet Mask**—The **Subnet Mask** for the destination network for which the route is being created
- **Gateway**—The next-hop gateway of the destination network for which the route is being created. The **Gateway** will be the IP address of the wireless interface of a SpeedNet Radio
- **Add**—After entering the details of the static route, click the **Add** button to add the route to the route table
- **Cancel**—Click the **Cancel** button to cancel the route creation process

Adding a Static Default Gateway

Clicking the **Add Default** button will add an **Add Default Gateway** section to the **Routing** tab. See Figure 75.

Figure 75. Add Default Gateway settings.

The **Gateway** field and **Add** and **Cancel** buttons are described below:

- **Gateway**—Enter the IP address of the next-hop gateway that will act as the default gateway for this SpeedNet Radio. The gateway will be the IP address of the wireless interface of a SpeedNet Radio
- **Add**—After entering the details of the default gateway, click the **Add** button to add the default gateway to the route table
- **Cancel**—Click the **Cancel** button to cancel the default gateway creation process

Persistent Routes

The **Persistent Routes** feature will establish a route to a specific destination before any application traffic is initiated. The **Persistent Routes** feature runs with **AODV** enabled and implements a keep-alive mechanism between a source and a destination.

The **Persistent Routes** feature is useful when traffic must keep flowing to specific paths in the network. It will also reduce delay and improve reliability between the nodes configured with the **Persistent Routes** feature.

It is important to note that entries for persistent routes only need to be configured in each end-point radio. No intermediate hops need to be entered. The AODV Mesh will automatically determine the route.

The following options are available:

- **Add**—The **Add** button is used to add persistent routes to the route table. Click the **Add** button, enter the Endpoint's IP address, and click the **OK** button to add a persistent route
- **Delete**—To delete a route from the route table, select the route, then click the **Delete** button to remove the route from the route table

IP Routing Window, ARP Tab

IP Address	MAC Address
192.168.213.101	00 FF FF 00 2E A5
192.168.213.104	00 FF FF 00 43 1B
192.168.213.107	00 FF FF 00 9C 44

Figure 76. The Address Resolution Protocol IP routing configuration window.

The Address Resolution Protocol (ARP) is used to associate an IP address to a device's corresponding MAC address. The **ARP** tab, shown in Figure 76, is used to view existing ARP table entries and to add or delete ARP table entries. The following parameters can be configured:

- **Address Resolution Protocol Table**—The **Address Resolution Protocol** table provides a list of current ARP entries. An ARP entry consists of two pieces of information: an IP address and a MAC address
- **IP Address**—To create a static ARP entry, enter the IP address of the device into the **IP Address** field

- **MAC Address**—Enter the MAC address of the device into the **MAC Address** field
- **Add**—After entering the IP address and MAC address into the corresponding fields, click the **Add** button to add the ARP entry to the Address Resolution Protocol
- **Delete**—To delete an ARP entry from the table, first select the entry. Click the **Delete** button to remove the entry from the ARP table

Note that most devices attached to a SpeedNet Ethernet port will automatically participate in ARP exchanges with the radio to associate their IP addresses with their MAC addresses. As such, it is unusual for SpeedNet Radio users to edit this table. The edit capability exists to enable IP communication from the SpeedNet Radios to/from devices that do not support ARP.

IP Routing Window, Blacklist Tab

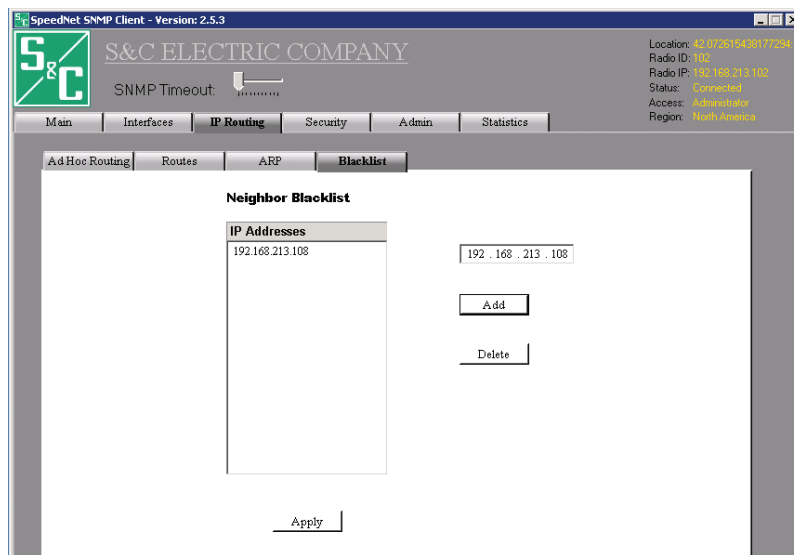


Figure 77. The IP routing configuration window.

The **Neighbor Blacklist** feature shown in Figure 77 allows the SpeedNet Client Tool to add, delete, and retrieve a blacklisted radio by using its IP address. A SpeedNet Radio address listed in the **Neighbor Blacklist** will not be considered a valid neighbor through which to build routes. The **Neighbor Blacklist** feature is used to prevent routing through SpeedNet Radios that qualify as valid neighbors but are neighbors that you do not want to use as next hop links for that particular radio address. One reason to exclude a neighbor is that it may have a permanent or transient line-of-sight impediment that results in poor packet delivery success over a given radio link. Further, that radio may not have a transmission problem from a different neighbor.

The **Neighbor Blacklist** address table is limited to a total 36 radio addresses.

The **Add** and **Delete** buttons are described below:

- **Add**—After entering an IP address, click the **Add** button to add the IP address to Neighbor Blacklist
- **Delete**—After selecting an IP address, click the **Delete** button to delete the IP address from the Neighbor Blacklist

Security Window, Encryption Tab

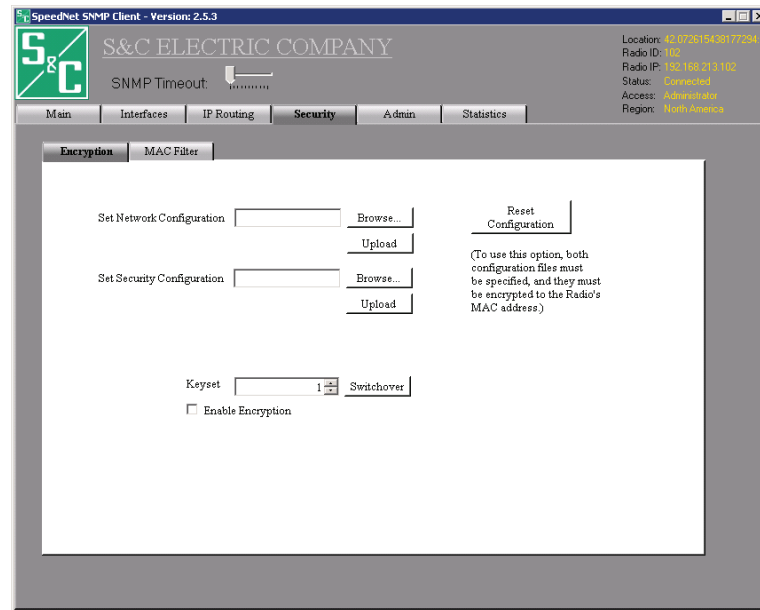


Figure 78. The Security encryption configuration window.

The **Security** window provides a list of tabs that can be used to view and set up the security configuration of the SpeedNet Radio. Selecting a tab will provide a list of configurable options.

The **Encryption** tab, shown in Figure 78, can be used to enable or disable encryption, change encryption keysets, and upload network and security configuration files. The following parameters can be configured:

- **Set Network Configuration**—After creating a network configuration file using the SpeedNet KeyGen Utility (see the “Network Configuration” section on page 22), this option allows administrators to upload the network-configuration file to the SpeedNet Radio. Click the **Browse** button to locate the network configuration file, which will have a .dat file extension. Click the **Upload** button to insert the network configuration into the SpeedNet Radio. Note that the network-configuration file loaded into a particular radio must either be encrypted with that radio’s MAC address (for initial configuration) or with a keyset loaded into that radio. You will be prompted to log in to the SpeedNet Client Tool after the network configuration has been applied. Note that after a radio is reset to the factory setting, the network configuration and/or setting the security configuration are the only actions allowed on that radio
- **Set Security Configuration**—After creating a security configuration (.rss) file using the SpeedNet KeyGen Utility (see “Generating a Security File” on page 17), this option allows administrators to upload the security configuration file to the SpeedNet Radio. Click the **Browse** button to locate the security configuration file, which will have an .rss file extension. Click the **Upload** button to insert the security configuration into the SpeedNet Radio. You will be prompted to log in after the security configuration has been applied. Note that after a radio is reset to factory settings, network configuration and/or setting security configuration are the only actions allowed for that radio
- **Keyset**—Specifies the encrypted keyset currently being used. All SpeedNet Radios within the network must use the same keyset in order to communicate with each other.
- **Use Latest**—Click the **Use Latest** button to use the keyset with the highest keyset number. All radios must use the same keyset in order to communicate

- **Switchover**—Enter the desired keyset number into the **Keyset** field, and click the **Switchover** button to use the new key
- SpeedNet Radios include an Auto Switchover feature that allows the network to automatically update to a more recent key. If a SpeedNet Radio receives a packet that was encrypted using a new keyset and the receiving radio has the new keyset installed, it will automatically switch to the new keyset. When switching keysets it is recommended to change the farthest radios first and work your way back to the closest radios
- **Enable Encryption**—Placing a checkmark in the **Enable Encryption** checkbox enables wireless network encryption on the SpeedNet Radio
- **Reset Configuration**—This feature is used to reset the configuration of a SpeedNet Radio

Security Window, MAC Filter Tab

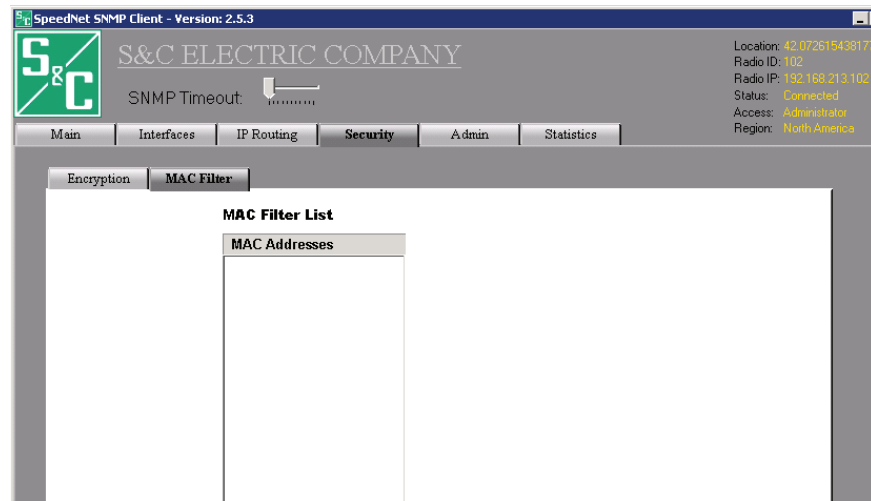


Figure 79. MAC Filter security configuration window.

The **MAC Filter** window, shown in Figure 79, can be used to view the list of MAC addresses that have been added to the MAC Address Revocation list using the SpeedNet KeyGen utility. There are no configurable parameters on the **MAC Filter** tab. All changes to the MAC Revocation list must be made using the SpeedNet KeyGen utility and uploaded to the SpeedNet Radio as part of a new security configuration file.

Admin Window, System Tab



Figure 80. The System Admin configuration window.

The **Admin** window has tabs that can be used to perform administrative tasks for the SpeedNet Radio that include upgrading firmware and determining system information. Selecting a tab will provide a list of configurable options.

The **System** tab, shown in Figure 80, is used to view system information, such as the current firmware version. System information, including radio ID and location, can be entered by the administrator. The following parameters can be configured:

- **MIB_Version**—This read-only field provides information regarding the current management information base (MIB) that is being used by the SNMP protocol
- **Firmware_Version**—This read-only field displays the current firmware version installed on the SpeedNet Radio
- **Running Time**—This read-only field displays the elapsed time since the last time the SpeedNet Radio was rebooted.
- **SpeedNet Radio ID**—Administrators can use this field to assign a descriptive name to the SpeedNet Radio. The SpeedNet Radio ID must consist of ASCII values but cannot contain spaces or the following characters: \$, ^, &, (, or)
- **System Name**— Administrators can use this field to assign a descriptive name to the entire network. The System ID must consist of ASCII values
- **System Location**— Administrators can use this field to note the location of the network. The System ID location must consist of ASCII values. The convention for location is for the system location to be in the form <signed decimal latitude>:<signed decimal longitude>. For example, a System Location of **33.578014746144: -101.865234375** is in Lubbock, Texas USA
- **System Contact**—Administrators can use this field to list the point of contact for the SpeedNet Radio network. The System ID must consist of ASCII values.
- **Apply**—Saves changes made to the configuration of the **System** tab. Changes will not be saved if you change to a different configuration tab without first clicking the **Apply** button
- **Reboot**—Clicking the **Reboot** button will cause the SpeedNet Radio to reboot

Admin Window, Firmware Tab

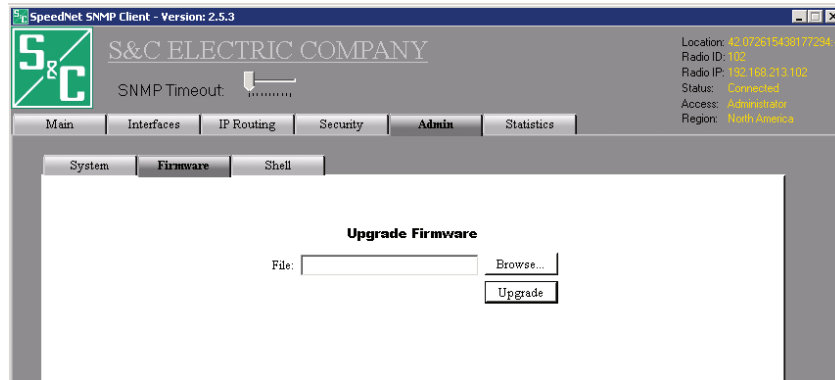


Figure 81. The Firmware admin configuration window.

The **Firmware** tab, shown in Figure 81, is used to upgrade the firmware installed on the SpeedNet Radio. The following parameters can be configured:

- **File**—Use the **Browse** button to specify the location of the firmware file to be uploaded
- **Upgrade**—After selecting the firmware file, click the **Upgrade** button to initiate an immediate firmware upgrade. The SpeedNet Radio will prompt for reboot at the conclusion of the upgrade. Power should not be cycled while a radio is upgrading firmware. You will need to log in to the radio again once the post-upgrade reboot is completed to do further work with the radio. It is recommended that users log in to the radio after the post-upgrade reboot and confirm the new firmware loaded by accessing the configuration window shown in Figure 80 on page 53

NOTICE

If the radio loses power during a firmware upgrade process, the radio will continue to use the firmware version that was installed before the attempted firmware upgrade.

Admin Window, Shell Tab

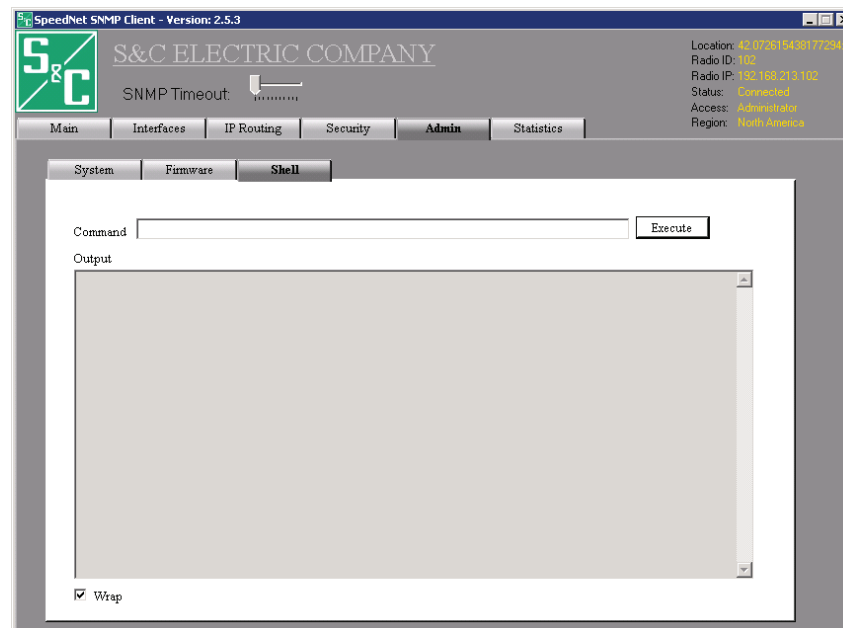


Figure 82. The Shell admin configuration window.

The **Shell** tab, shown in Figure 82 on page 54, is provided to support advanced integrator troubleshooting and is not used for configuration of a SpeedNet Radio network. A limited selection of LINUX shell commands (e.g. `cat`, `cd`, `ls`) can be executed. Execution of shell commands is performed in a batch manner, waiting for the output to complete before returning a result. As such, execution of commands that produce continuing output (e.g. default LINUX ping command) will “hang” the shell command in the client tool without ever returning a result.

Here are some useful shell commands and their descriptions. Note that shell commands are for advanced users, and they are not guaranteed to carry forward into future versions of SpeedNet Radio firmware. These shell commands lack the automated range and other check features of the SpeedNet Client Tool GUI.

NOTE: Shell commands have the potential to lock up radios in a state that requires power cycling or (worse) a state that prevents them from rebooting successfully. Because of this, shell commands should be used with caution.

- **`cat /etc/config/config.dat`**—Prints the configuration file; users can copy and paste the result into another tool (e.g. Windows Notepad) to create a record of radio configurations
- **`cat /proc/aodv/neighbor`**—Prints the AODV neighbor list; users can copy and paste the result into another tool (e.g. Windows Notepad) to create a record of radio neighbors that can greatly aid in determining the connectivity in the SpeedNet mesh
- **`head -n <count> /etc/config/config.dat`**—Views the first few `<count>` lines of the configuration file
- **`tail -n <count> /etc/config/config.dat`**—Views the last `<count>` lines of the configuration file
- **`ping -c <count> <host IP>`**—Pings the host indicated by `<host IP>`; the number of ping requests sent is controlled by `<count>`, and the SpeedNet Radio does not use DNS, so `<host IP>` must be a standard dotted-number notation IP address (e.g., 192.168.200.1)

It is important that a value for `<count>` actually be set. Until the ping command has completed execution (approximately `<count>` seconds) the radio will not respond to further SNMP requests. If `<count>` is not set (i.e., if the `-c` option is not provided), the ping command will not return and the radio will not answer SNMP requests until it is rebooted. Because the radio cannot answer SNMP requests (such as reboot requests), the only way to reboot will be to cycle power physically at the radio. Power cycling radios installed in the field is a significant effort

- **`/sbin/route | grep <host IP>`**—Print the route to `<host IP>`, if it exists. If this command returns nothing, it means no route to the indicated host exists. The line between “route” and “grep” is a vertical bar and on most keyboards is generated by holding the Shift key and pressing the backslash key

Statistics Window, Ethernet Tab

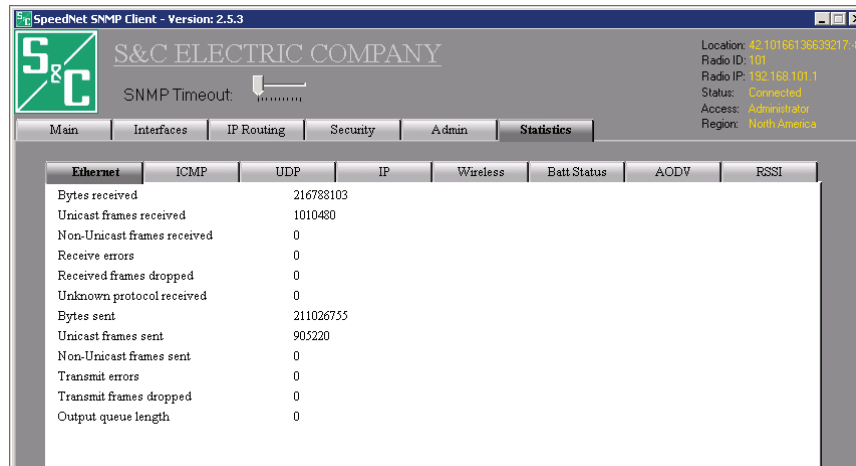


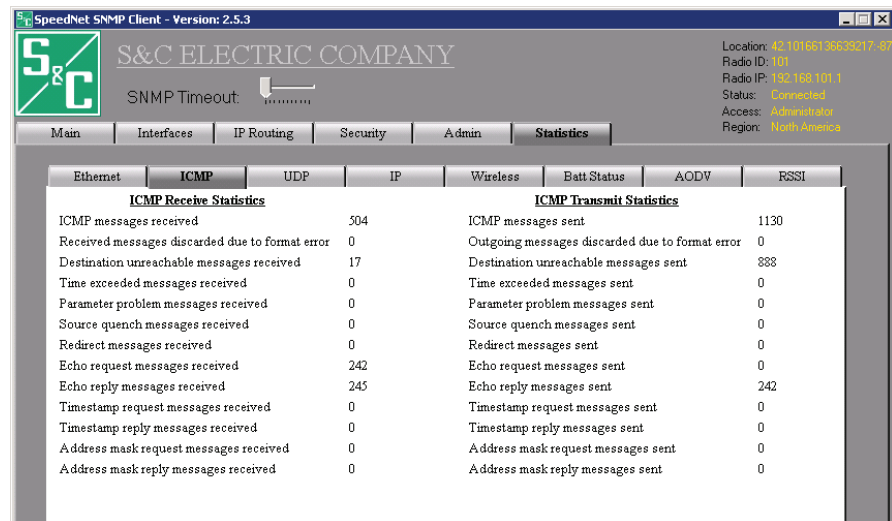
Figure 83. The Ethernet statistics window.

The **Statistics** window has several tabs that provide statistical information regarding interface traffic, protocol data, and routing. This section contains descriptions of each statistic that is available through the SpeedNet Client Tool.

The **Ethernet** tab, shown in Figure 83, provides the following statistical information regarding the performance of the SpeedNet Radio's Ethernet interface:

- **Bytes received**—Total number of bytes received by the SpeedNet Radio's Ethernet interface; the bytes received, together with the bytes sent, represent the total data transfer of all communications links involving the Ethernet interface
- **Unicast frames received**—The total number of single destination (unicast) frames sent to the SpeedNet Radio's Ethernet interface
- **Non-Unicast frames received**—The total number of non-unicast frames sent to the SpeedNet Radio's Ethernet interface
- **Receive errors**—The total number of receive errors
- **Received frames dropped**—The total number of frames received by the SpeedNet Radio's Ethernet interface that were discarded
- **Unknown protocol received**—The total number of frames received by the SpeedNet Radio's Ethernet interface with unidentified protocol errors
- **Bytes sent**—The total number of bytes sent by the SpeedNet Radio's Ethernet interface
- **Unicast frames sent**—The total number of single destination (unicast) frames sent from the SpeedNet Radio's Ethernet interface
- **Non-Unicast frames sent**—The total number of non-unicast frames sent from the SpeedNet Radio's Ethernet interface
- **Transmit errors**—The total number of transmit errors; this error is received from the application device and may indicate a problem with the IntelliRupter fault interrupter
- **Transmit frames dropped**—The total number of frames transmitted and then discarded; this error is received from the application device and may indicate a problem with the IntelliRupter fault interrupter
- **Output queue length**—An error received from the application device that may indicate a problem with the IntelliRupter fault interrupter on the application device that may indicate a problem with the IntelliRupter

Statistics Window, ICMP Tab



The ICMP Tab, as shown in Figure 84, provides the following statistical information regarding the Internet Control Message Protocol:

- **ICMP messages sent**—The total number of ICMP messages sent by the radio
- **Outgoing messages discarded due to format error**—The total number of ICMP messages sent by a radio that were not delivered because of format errors
- **Destination unreachable messages sent**—The total number of destination unreachable messages sent by the radio; destination unreachable messages are generated when the destination address is unreachable
- **Time exceeded messages sent**—The total number of messages sent by the radio that exceeded their time to live
- **Parameter problem messages sent**—The total number of parameter problem messages sent; a parameter problem message is sent when an error in the IP header of a datagram is detected
- **Source quench messages sent**—The total number of source quench messages sent by the radio; a source quench request is sent to request a reduction in the packet transmission rate
- **Redirect messages sent**—The total number of redirect messages sent; a redirect is sent when an alternate route for the datagram is selected
- **Echo request messages sent**—The total number of echo requests sent; an echo request causes the receiving radio to send an echo reply message back to the originating radio, and echo requests are typically generated by a “Ping” application
- **Echo reply messages sent**—The total number of echo replies sent; an echo reply is sent to respond to an echo request, and echo replies are typically generated by a “Ping” application
- **Timestamp request messages sent**—The total number of timestamp requests sent; a timestamp request causes the radio to send a timestamp reply to the originating radio
- **Timestamp reply messages sent**—The total number of timestamp replies sent; a timestamp reply is sent in response to a timestamp request, and timestamp replies and requests measure the transmission speed of datagrams on a network
- **Address mask request messages sent**—The total number of address mask requests sent; an address mask request is sent to determine the number of bits in the subnet mask for the destination’s Ethernet subnet
- **Address mask reply messages sent**—The total number of address mask responses sent; an address mask response is sent in response to an address mask request

Statistics Window, UDP Tab

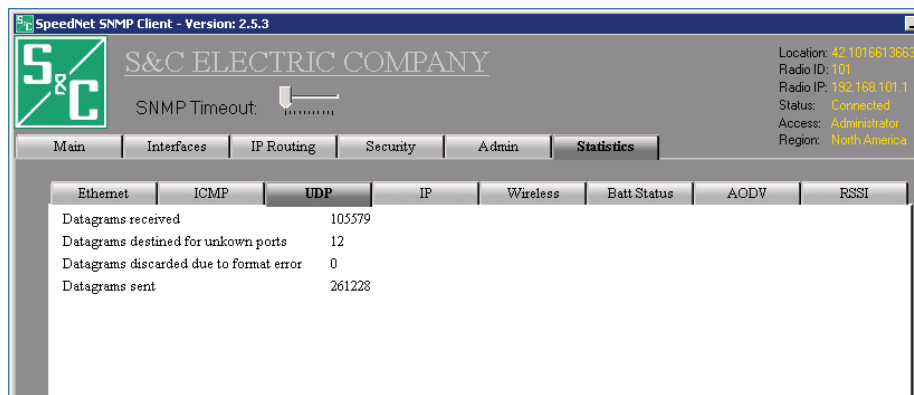


Figure 85. The User Data Protocol statistics window.

The UDP tab, as shown in Figure 85, provides the following statistical information regarding the User Datagram Protocol. UDP is generated by the application layer and uses ports to facilitate application-to-application communication:

- **Datagrams received**—The total number of UDP datagrams successfully received
- **Datagrams destined for unknown ports**—The total number of received UDP datagrams with unknown destination ports
- **Datagrams discarded due to format error**—The total number of UDP datagrams that were not delivered because of format errors
- **Datagrams sent**—The total number of UDP datagrams sent

Statistics Window, IP Tab

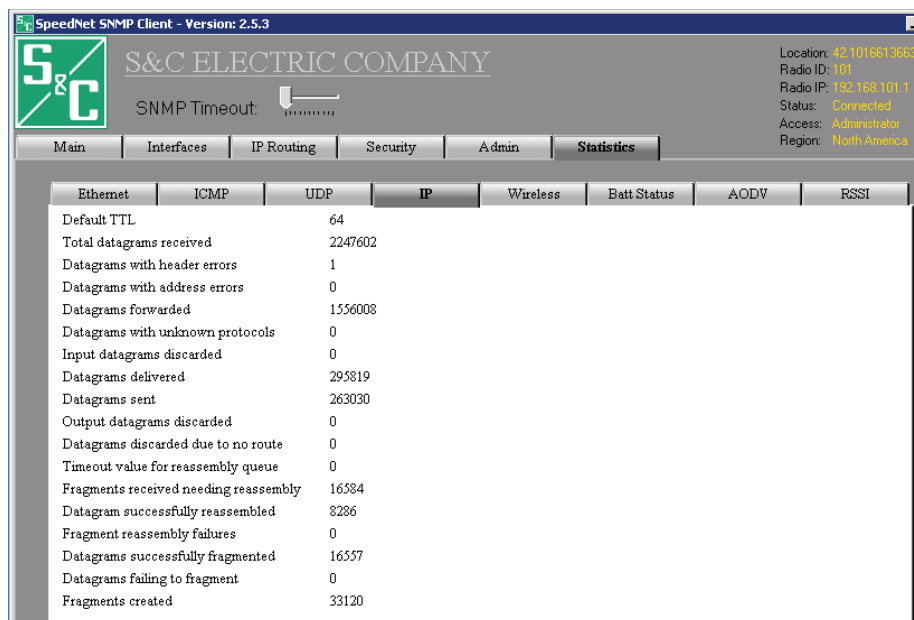


Figure 86. The Internet Protocol statistics window.

The IP tab, as shown in Figure 86, provides the following statistical information regarding the Internet Protocol:

- **Default TTL**—The time-to-live value used to determine how long a packet that has not reached its destination will remain on the network prior to be discarded
- **Total datagrams received**—The total number of IP data packets received
- **Datagrams with header errors**—The total number of received IP data packets that contain errors in the header, such as incorrect IP header length

- **Datagrams with address errors**—The total number of received IP data packets that contain address errors
- **Datagrams forwarded**—The total number of IP data packets forwarded because the receiving radio was not the intended destination
- **Datagrams with unknown protocols**—The total number of data packets received with protocols not recognized by the radio
- **Input datagrams discarded**—The total number of IP data packets received that were discarded because the node was too busy
- **Datagrams delivered**—The total number of IP data packets successfully delivered to the destination application
- **Datagrams sent**—The total number of IP data packets sent
- **Output datagrams discarded**—The total number of data packets sent that were discarded because the node was too busy
- **Datagrams discarded due to no route**—The total number of data packets discarded because of the lack of correct routing information
- **Timeout value for reassembly queue**—The duration before the reassembly queue is cleared and the connection is dropped
- **Fragments received needing reassembly**—The total number of received IP data packet fragments that require reassembly; if a data packet cannot be sent in a single transmission, it will be broken into fragments and then reassembled upon receipt
- **Datagrams successfully reassembled**—The total number of fragmented IP data packets received and reassembled
- **Fragment reassembly failures**—The total number of fragmented IP data packets received that could not be reassembled
- **Datagrams successfully fragmented**—The total number of IP data packet fragments generated
- **Datagrams failing to fragment**—The total number of data packets discarded because the fragmentation process failed to fragment the packets
- **Fragments created**—The total number of IP data packet fragments created

Statistics Window,
Wireless Tab



Figure 87. The Wireless statistics window.

The **Wireless** tab, shown in Figure 87, provides the following statistical information regarding the wireless performance of the SpeedNet Radio:

- **Bytes received**—The total number of bytes successfully received by the SpeedNet Radio wireless interface
- **Packets received**—The total number of packets successfully received by the SpeedNet Radio wireless interface
- **Received packets dropped**—The total number of packets received by the SpeedNet Radio wireless interface that failed the validation check for problems such as a corrupted CRC
- **Packets received with bad length**—The total number of packets received by the SpeedNet Radio wireless interface that contained checksum errors involving length
- **Packets received with bad CRC**—The total number of packets received by the SpeedNet Radio wireless interface that contained checksum errors
- **Bytes transmitted**—The total number of bytes transmitted over the SpeedNet Radio wireless interface
- **Packets transmitted**—The total number of packets transmitted over the SpeedNet Radio wireless interface
- **Packets repeated**—The number of repeated packet transmissions; if a transmission

Statistics Window,
Battery Status Tab

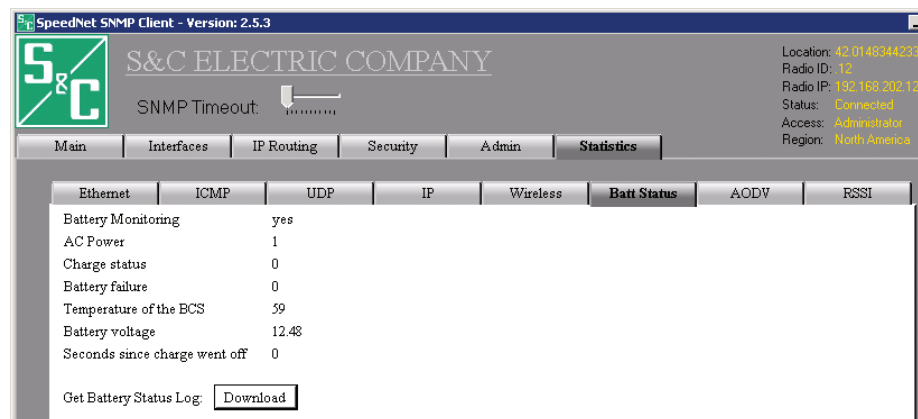


Figure 88. The Battery Status statistics window.

The **Battery Status** tab, shown in Figure 88, provides the following statistical information regarding the battery performance when a battery is connected to the SpeedNet Radio:

- **Battery Monitoring**—Indicates whether Battery Monitoring has been activated; battery monitoring is enabled by placing a checkmark next to the Enable Battery Testing option, which is located on the **Serial Mode** tab of the Interfaces configuration page
- **AC Power**—1 = ON, 0 = OFF

- **Charge status**—Charger status flag: the charger has a malfunction when the flag is True/1, and the charger is OK when the flag is False/0
- **Battery failure**—Battery status flag: the battery is not fully functional when the flag is True/1, and the battery is OK when the flag is False/0
- **Temperature of BC**—Internal temperature of the SpeedNet Radio, in °F
- **Battery voltage**—This value should be 12 to 13 volts unless the battery is discharging
- **Seconds since charge went off**—Duration since ac power has been removed
- **Get Battery Status Log**—Press the **Download** button to save the battery status statistics as a text file

Statistics Window, AODV Tab

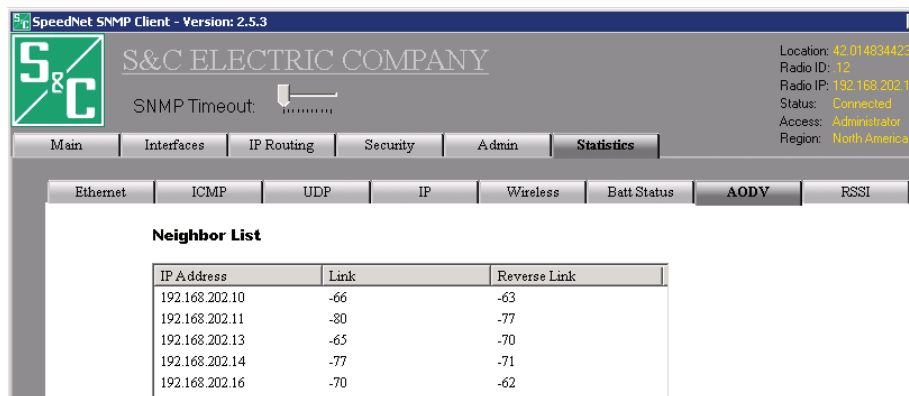


Figure 89. The AODV statistics window.

The **AODV** tab, shown in Figure 89, provides statistical information regarding the link quality between all SpeedNet Radios within the wireless communication range of the local SpeedNet Radio. The **AODV statistics** tab is only active when the AODV ad-hoc routing protocol has been enabled on the **Ad Hoc Routing** tab of the IP Routing configuration page.

The Neighbor List provides a list of SpeedNet Radios that are communicating wirelessly with the local SpeedNet Radio. The Neighbor List is updated each time a “Hello” message is received from another SpeedNet Radio.

The column headings for Neighbor List are described below:

- **IP Address**—This field provides the IP address of the wireless interface of a SpeedNet Radio whose “Hello” message has been received by the local SpeedNet Radio
- **Link**—Provides a measurement of the local SpeedNet Radio signal strength as measured by the remote SpeedNet Radio and specified by the IP address that sent the “Hello” message. This is used to ensure only bidirectional links are used for routing wireless data packets. A bidirectional link will show both Link and Reverse Link signal strengths in this Neighbor List. A unidirectional link is indicated when hello beacons are received from a remote SpeedNet Radio that do not contain the local radio’s IP address and corresponding measurement of the local radio’s received signal strength as received at the remote radio. A unidirectional link will not have a Link entry in this Neighbor List
- **Reverse Link**—Provides a measurement of the signal strength of the last “Hello” message that was received from the SpeedNet Radio. The Reverse Link measurement is provided in dBm

Statistics Window, RSSI Tab

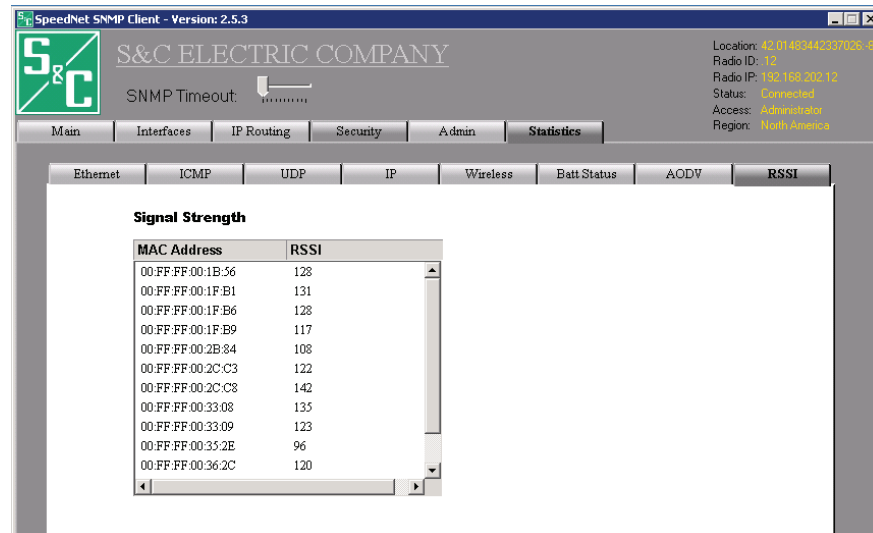


Figure 90. The RSSI statistics window.

The **RSSI** tab, shown in Figure 90, provides the statistical information regarding the link signal strength between all SpeedNet Radios within wireless communication range of the local SpeedNet Radio. The **Received Signal Strength Indicator** tab lists SpeedNet Radios based on their unique MAC address. Unlike the AODV Neighbor List, the **RSSI** tab does not require an exchange of Hello beacons.

The column headings for Signal Strength are described below:

- **MAC Address**—This displays the MAC Address of the SpeedNet Radio whose signal RSSI value is displayed
- **RSSI**—The RSSI (Received Signal Strength Indication) field provides a measurement of the current RSSI based on the last packet that was received from the destination radio. RSSI values have a range of 0-255, with larger values equating to better signal strength