Contents

[Disclaimer 2](#_Toc535518839)

[Version History 3](#_Toc535518840)

[Operation 4](#_Toc535518841)

[Overview 4](#_Toc535518842)

[Load 5](#_Toc535518843)

[Zeroize 6](#_Toc535518844)

[Read 7](#_Toc535518845)

[RS-232 Serial Driver 8](#_Toc535518846)

[Windows 10 9](#_Toc535518847)

[Installation 9](#_Toc535518848)

[Connection 41](#_Toc535518849)

[Disconnection 49](#_Toc535518850)

[License 55](#_Toc535518851)

[Manual Revision History 56](#_Toc535518852)

# Disclaimer

This utility is not intended for use in a production setting – security was not a consideration of the design. If you are operating a production system, use a commercial keyloader that supports P25 link layer authentication.

The subscriber identity and the link layer authentication key loaded into to the radio need to be entered into the trunking system in order for the authentication process to be successful. This tool by itself will not allow access to a link layer authentication protected trunking system.

# Version History

|  |  |  |
| --- | --- | --- |
| **Version #** | **Date** | **Description** |
| 1.0.0.0 | 2019-01-17 | Initial Release |

# Operation

## Overview

This utility is a Windows .NET Console Application that implements all Manual Rekeying Features for Authentication per TIA-102.AACD-A.

The Microsoft .NET Framework 4.6.1 (or later) is required to be installed.

The following command line flags are available:

|  |  |
| --- | --- |
| -h, -?, --help | show help and exit |
| -q, --quiet | do not show output |
| -v, --verbose | show debug messages |
| -i, --ip=VALUE | radio ip address [default 192.168.128.1] |
| -p, --port=VALUE | radio udp port number [default 49165] |
| -t, --timeout=VALUE | radio receive timeout (ms) [default 5000] |
| -l, --load | load key |
| -z, --zeroize | zeroize key(s) |
| -r, --read | read key(s) |
| -d, --device | device scope |
| -a, --active | active scope |
| -n, --named | named scope |
| -w, --wacn=VALUE | wacn id (hex) |
| -s, --system=VALUE | system id (hex) |
| -u, --unit=VALUE | unit id (hex) |
| -k, --key=VALUE | aes-128 encryption key (hex) |

The /wacn, /system, and /unit, and /key flags all expect hex values.

If the load action is specified, the key is required.

If the named scope is specified, the WACN ID, System ID, and Unit ID are required.

Radio IP 192.168.128.1 and UDP port 49165 are the default. This combination is used by Motorola radios, however other vendors may be different. Connection over PPP (through the RS-232 serial driver) or over RNDIS is supported, as that configuration is on the Windows level.

## Load

This action loads a key into the radio by sending a ‘Load Authentication Key Command’ KMM.

Only the active and named scopes are supported.

Example: Load the link layer authentication key 0x000102030405060708090A0B0C0D0E0F into the active subscriber identity.

sakl.exe /load /active /key 000102030405060708090a0b0c0d0e0f

Example: Load the link layer authentication key 0x000102030405060708090A0B0C0D0E0F into the subscriber identity defined by WACN ID: 0xA4398, System ID: 0xF10, Unit ID: 0x99B584.

sakl.exe /load /named /wacn a4398 /system f10 /unit 99b584 /key 000102030405060708090a0b0c0d0e0f

This action returns 0 if the operation completed successfully, or -1 if there was an error during the operation.

## Zeroize

This action deletes key(s) in the radio by sending a ‘Delete Authentication Key Command’ KMM.

Example: Delete all link layer authentication keys in the device.

sakl.exe /zeroize /device

Example: Delete the link layer authentication key associated with the active subscriber identity.

sakl.exe /zeroize /active

Example: Delete the link layer authentication key associated with the subscriber identity defined by WACN ID: 0xA4398, System ID: 0xF10, Unit ID: 0x99B584.

sakl.exe /zeroize /named /wacn a4398 /system f10 /unit 99b584

This action returns 0 if the operation completed successfully, or -1 if there was an error during the operation.

## Read

This action lists the status of the key(s) in the radio by sending an ‘Inventory Command (List Active SUID)’ KMM.

Only the device and active scopes are supported.

NOTE: This does not read the encryption key itself, but the status of the key.

Example: List all link layer authentication keys in the device.

sakl.exe /read /device

Example: List the link layer authentication key associated with the active subscriber identity.

sakl.exe /read /active

The following information is printed for each key returned by the device:

WACN: 0xA4398, System: 0xF10, Unit: 0x99B584, Key Assigned: True, Is Active: True

This action returns 0 if the operation completed successfully, or -1 if there was an error during the operation.

# RS-232 Serial Driver

NOTE: The driver connects 9600 bits per second, 8 data bits, no parity bit, 1 stop bit (9600-8-N-1) by default. In order to change baud rates, the DCB entry in the INF file has to be changed.

IMPORTANT: Start with the radio disconnected from the serial port. This prevents Windows from automatically starting the connection before the configuration is complete.

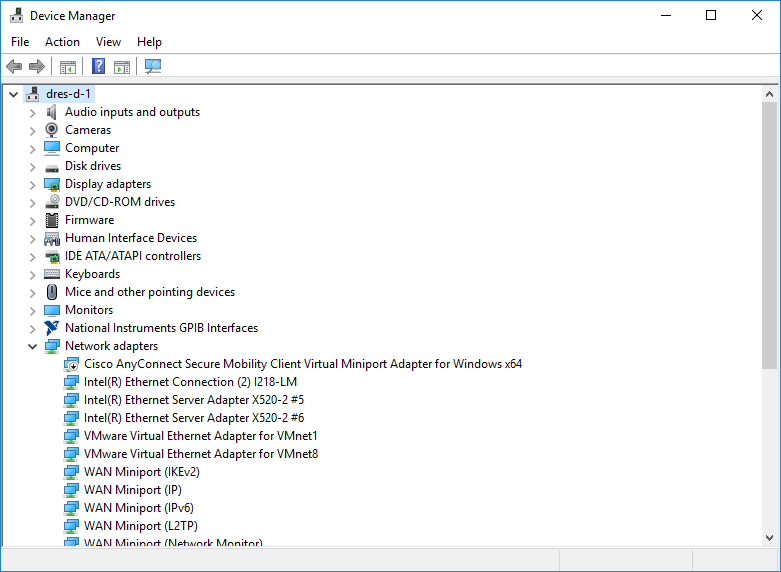
## Windows 10

NOTE: The following depicts Windows 10 Enterprise, 64-bit, Build 1803. Steps on earlier or later builds may differ.

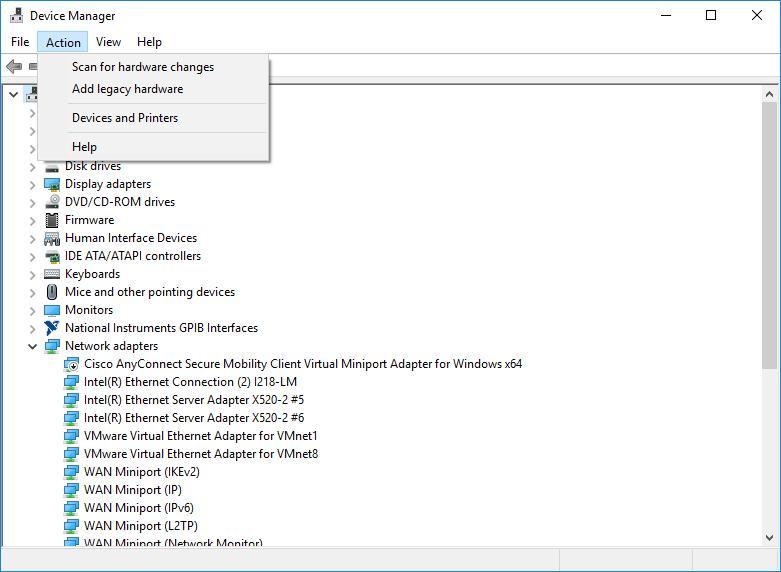
### Installation

Open Device Manager.

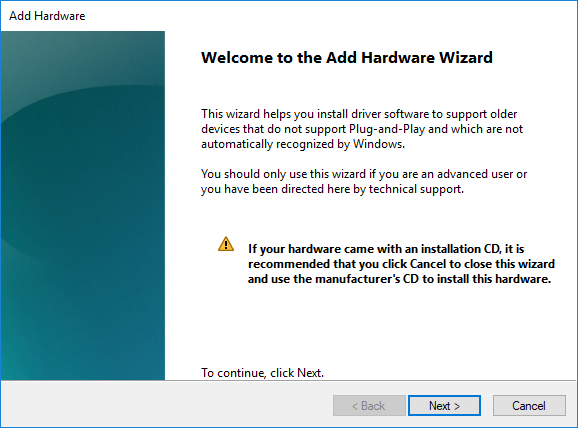
Click on the computer name.



Click the ‘Action’ menu, then ‘Add legacy hardware’.

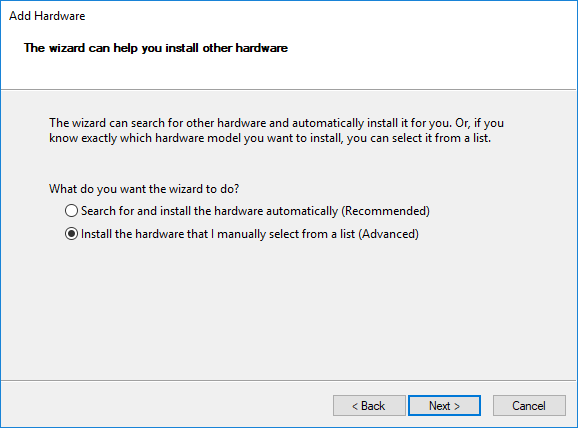


Click ‘Next’.



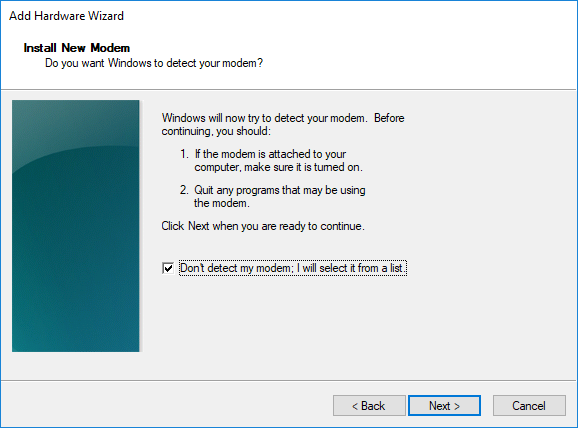
Select ‘Install the hardware that I manually select from a list (Advanced)’.

Click ‘Next’.

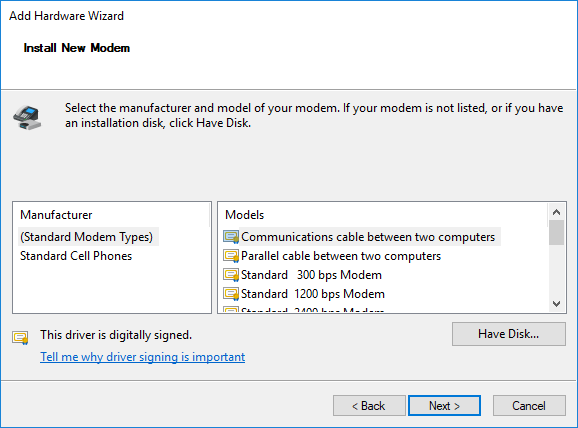


Select the ‘Don’t detect my modem; I will select it from a list’ option.

Click ‘Next’.

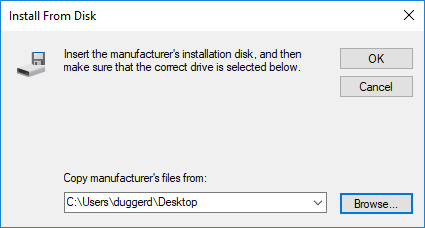


Click ‘Have Disk’.



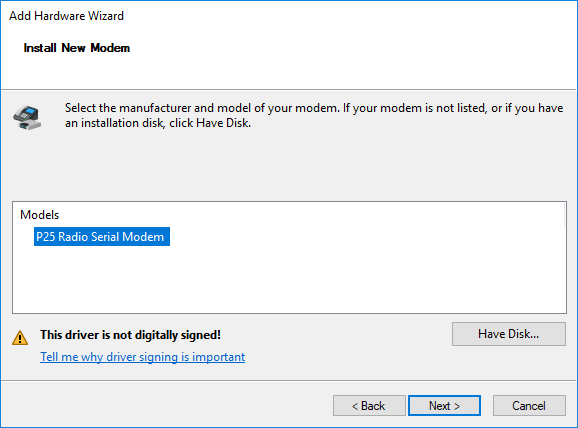
Click ‘Browse’ and navigate to the folder that contains the ‘P25RadioSerialModem.inf’ file.

Click ‘OK’.



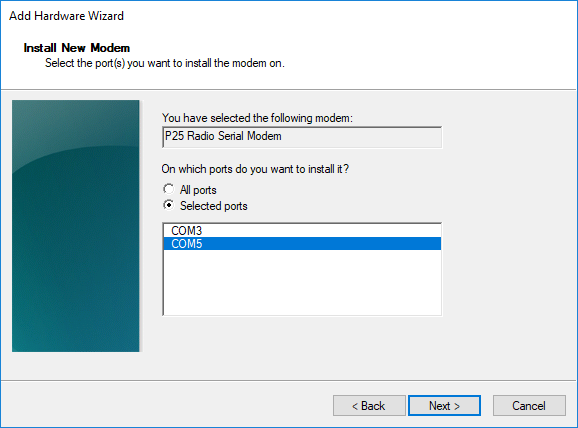
Select ‘P25 Radio Serial Modem’.

Click ‘Next’.

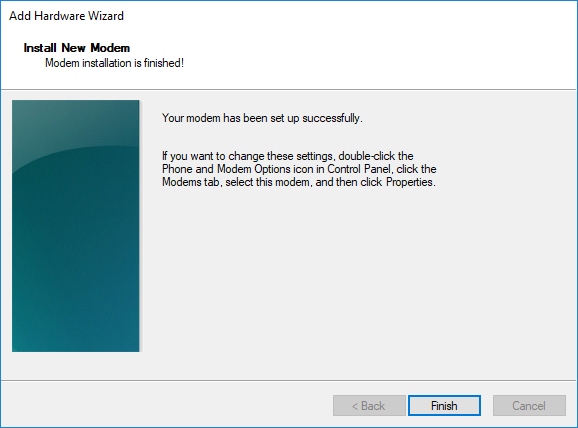


Select the COM port that is connected to the radio.

Click ‘Next’.

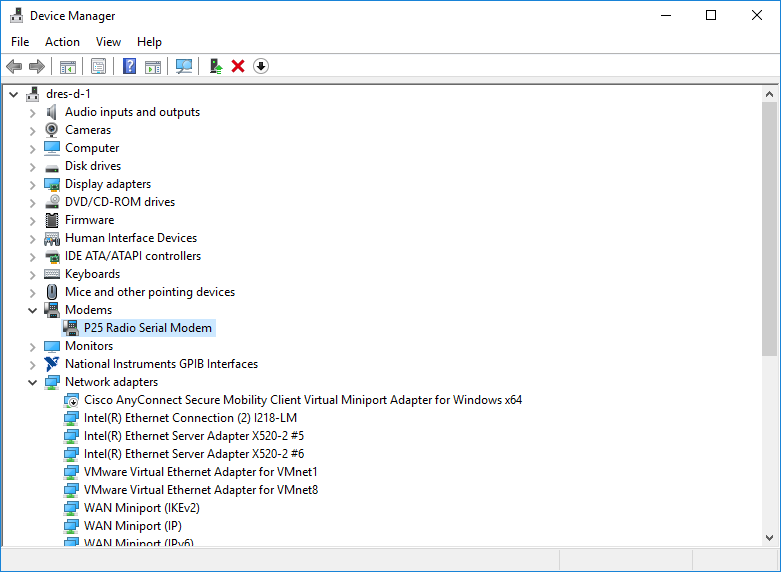


Click ‘Finish’.



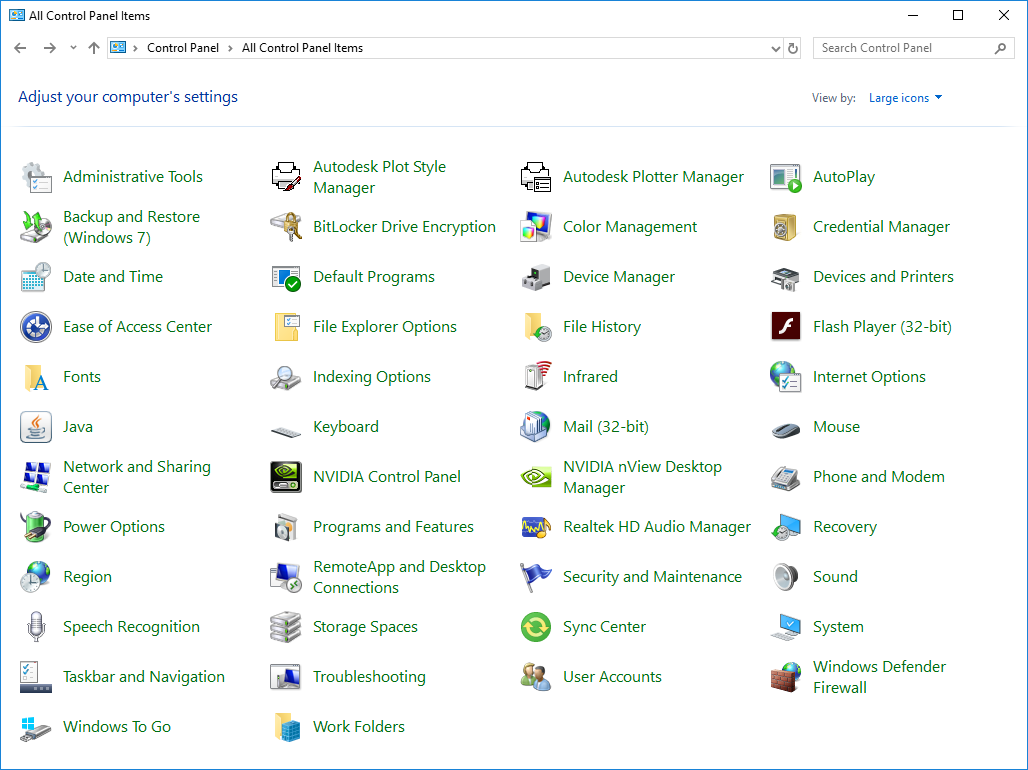
Verify that the ‘P25 Radio Serial Modem’ item appears under the ‘Modems’ category.

You may have to select ‘Action’->’Scan for hardware changes’ for the modem to appear.



Open the Control Panel.

Click ‘Phone and Modem’.

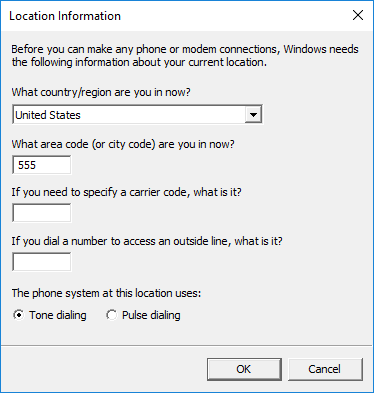


If this window appears:

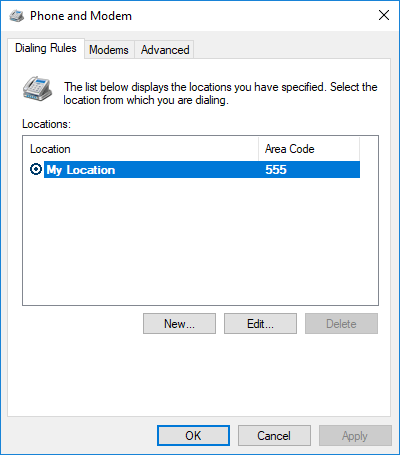
Select ‘United States’ from the ‘What country/region are you in now?’ combo box.

Enter ‘555’ into the ‘What area code (or city code) are you in now?’ text box.

Click ‘OK’.

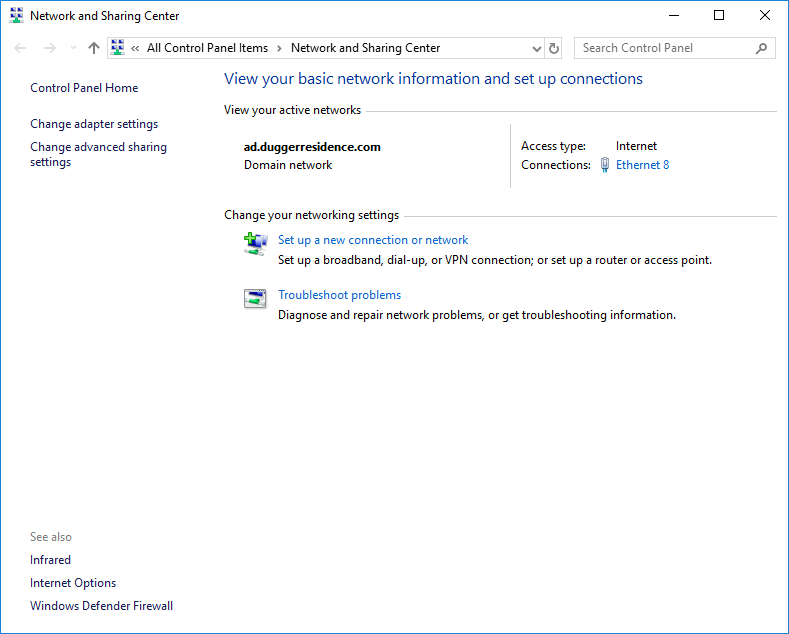


Click ‘OK’.



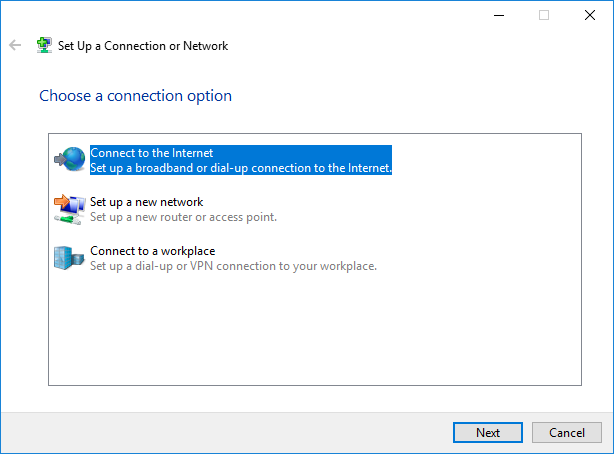
Open the Network and Sharing Center.

Click ‘Set up a new connection or network’.

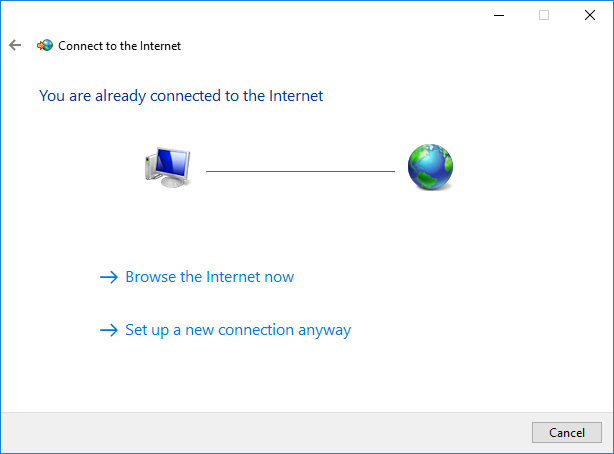


Select ‘Connect to the Internet’.

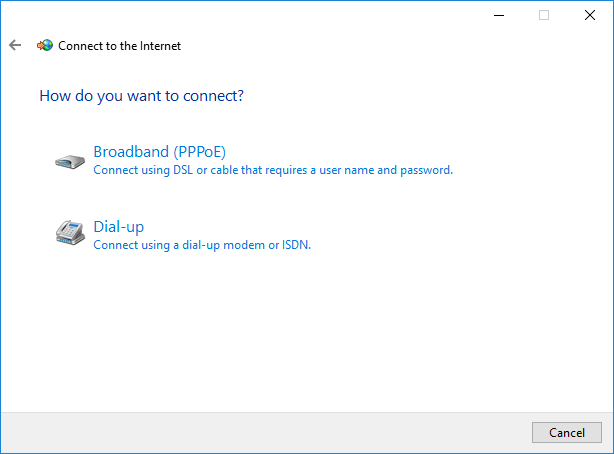
Click ‘Next’.



Click ‘Set up a new connection anyway’.



Click ‘Dial-up’.

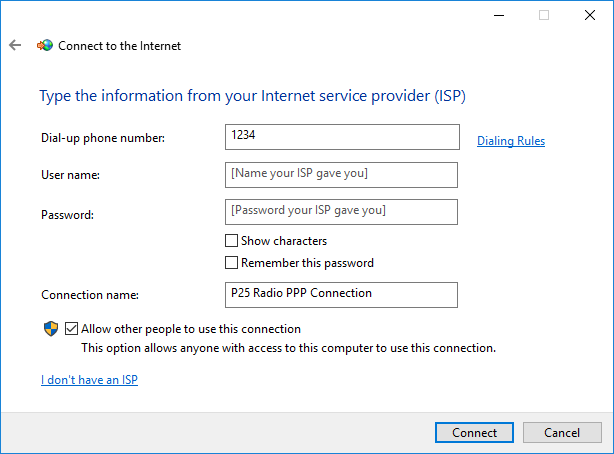


Enter ‘1234’ (or any number) into the ‘Dial-up phone number’ text box.

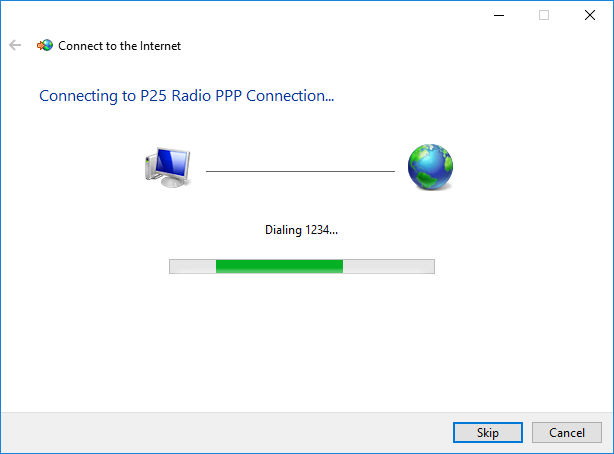
Enter ‘P25 Radio PPP Connection’ (or any name) into the ‘Connection name’ text box.

Select ‘Allow other people to use this connection.

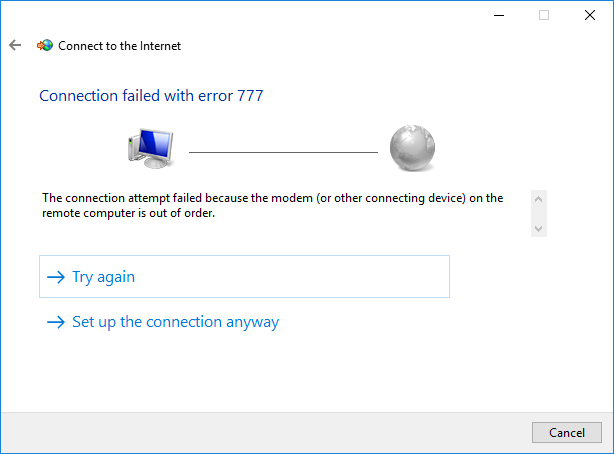
Click ‘Connect’.



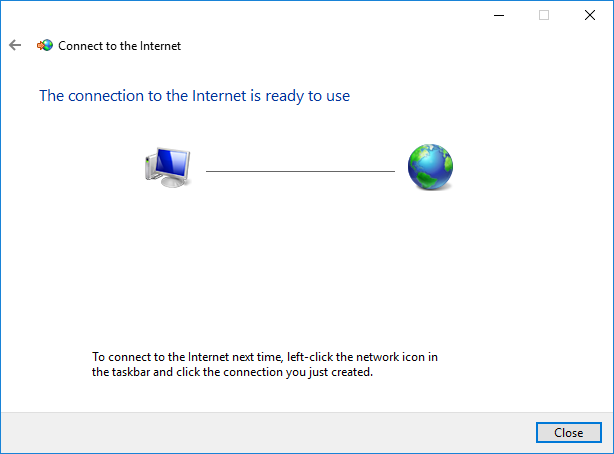
Click ‘Skip’.



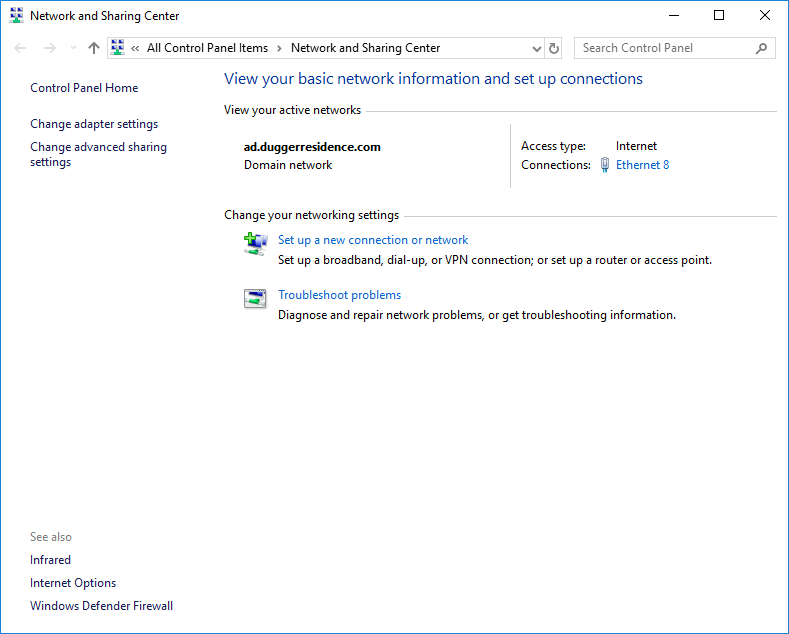
If this message appears, click ‘Set up the connection anyway’.



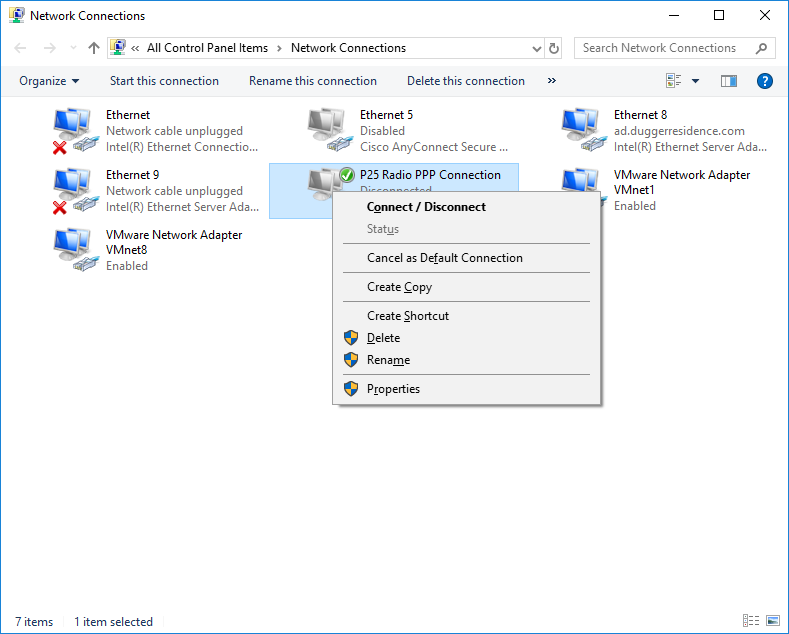
Click ‘Close’.



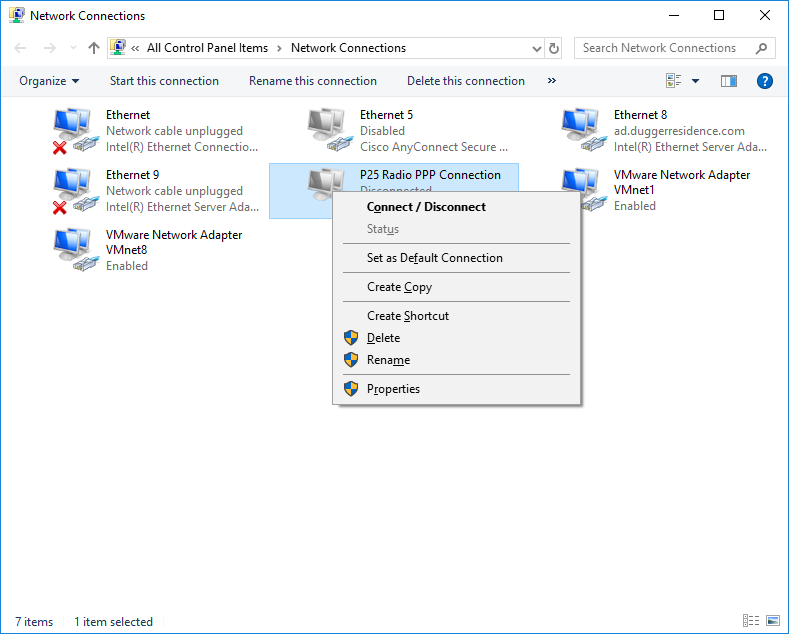
Click ‘Change Adapter Settings’



Right click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection), and click ‘Cancel as Default Connection’.



Right click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection), and click ‘Properties’.

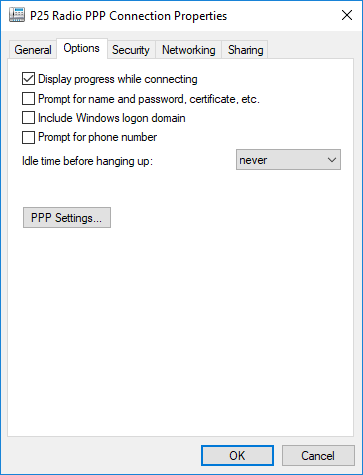


Click ‘Options’

Uncheck ‘Prompt for name and password, certificate, etc’.

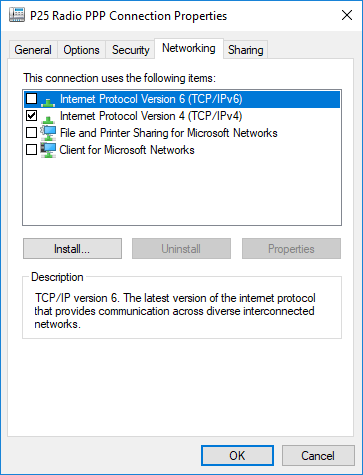
Uncheck ‘Prompt for phone number’.

Select ‘never’ from the ‘Idle time before hanging up’ combo box.



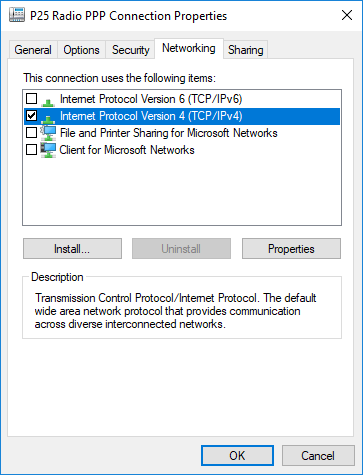
Click ‘Networking’

Uncheck ‘Internet Protocol Version 6 (TCP/IPv6)’.

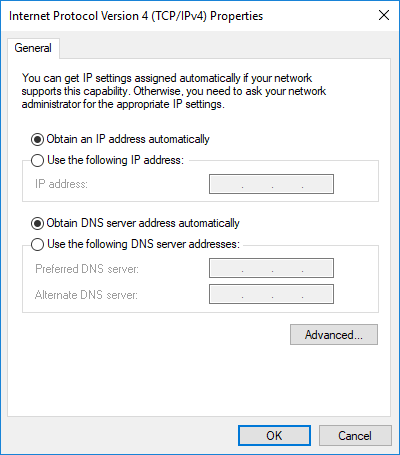


Click ‘Internet Protocol Version 4 (TCP/IPv4)’.

Click ‘Properties’.

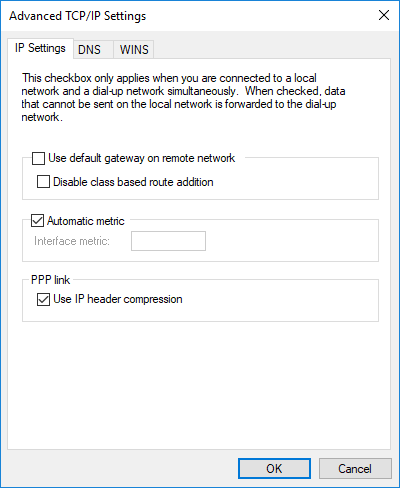


Click ‘Advanced’.

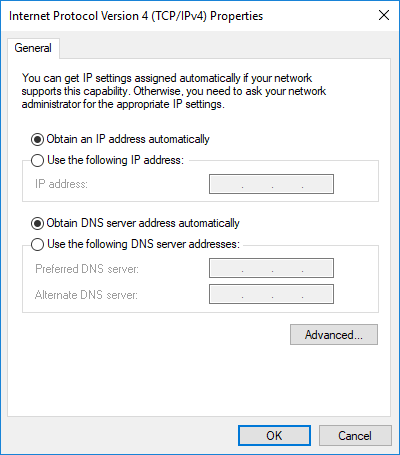


Uncheck ‘Use default gateway on remote network’.

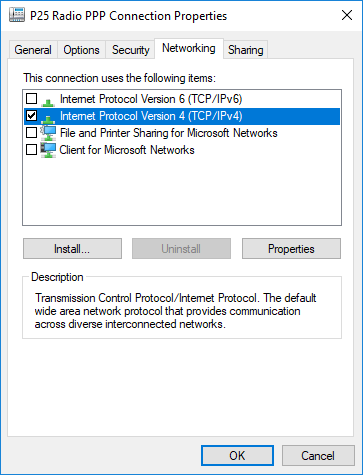
Click ‘OK’.



Click ‘OK’.



Click ‘OK’.

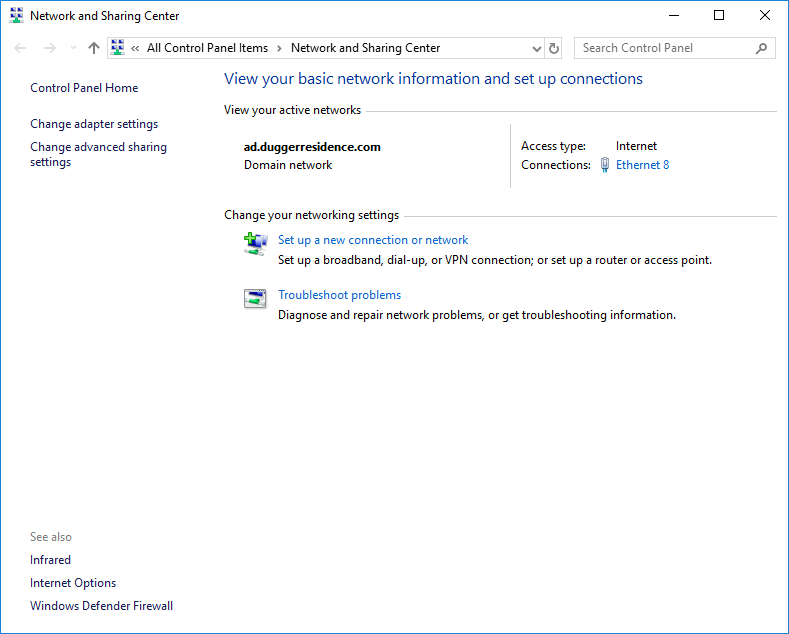


### Connection

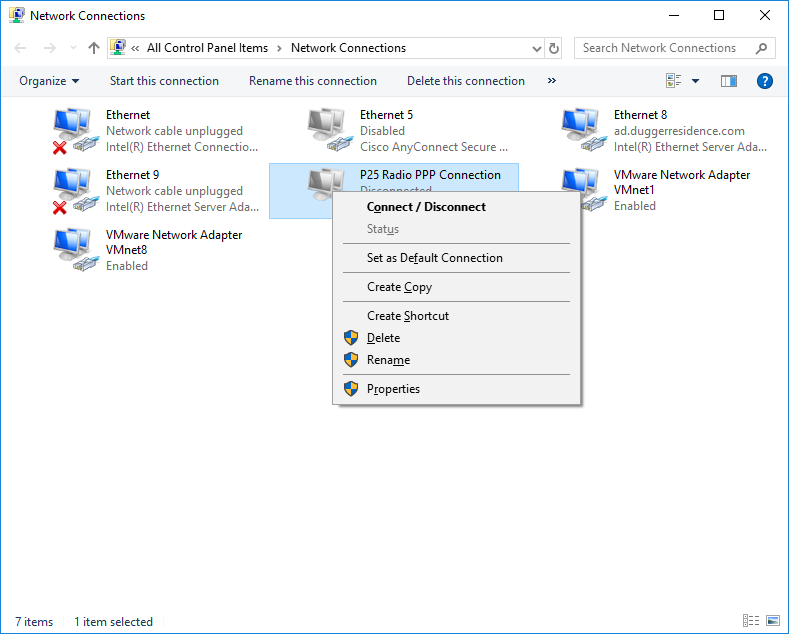
Connect the radio to the serial port.

Open the Network and Sharing Center.

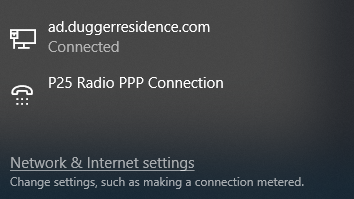
Click ‘Change Adapter Settings’.



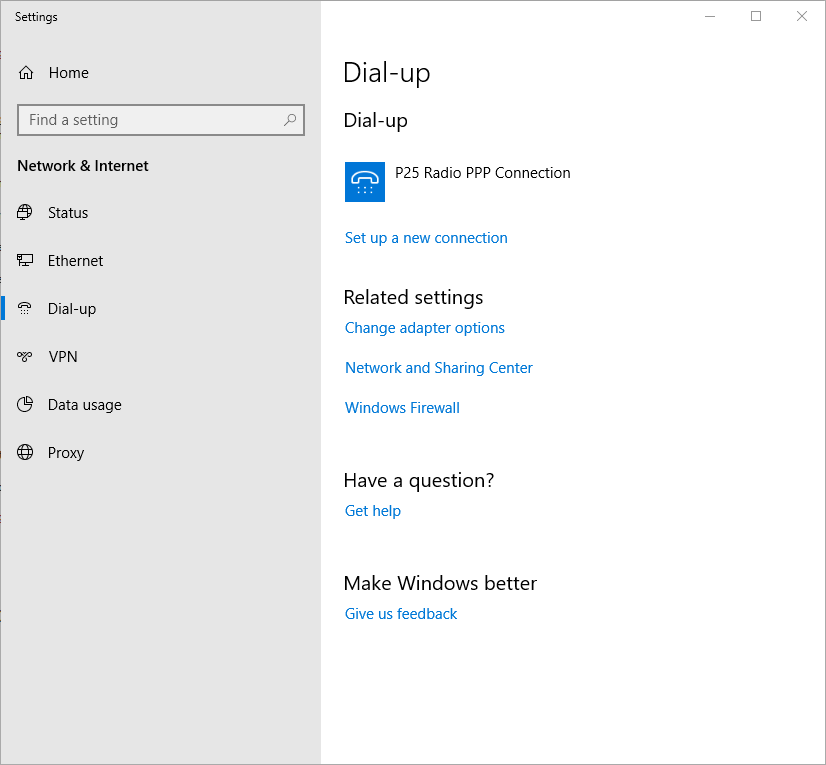
Right click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection), and click ‘Connect / Disconnect.



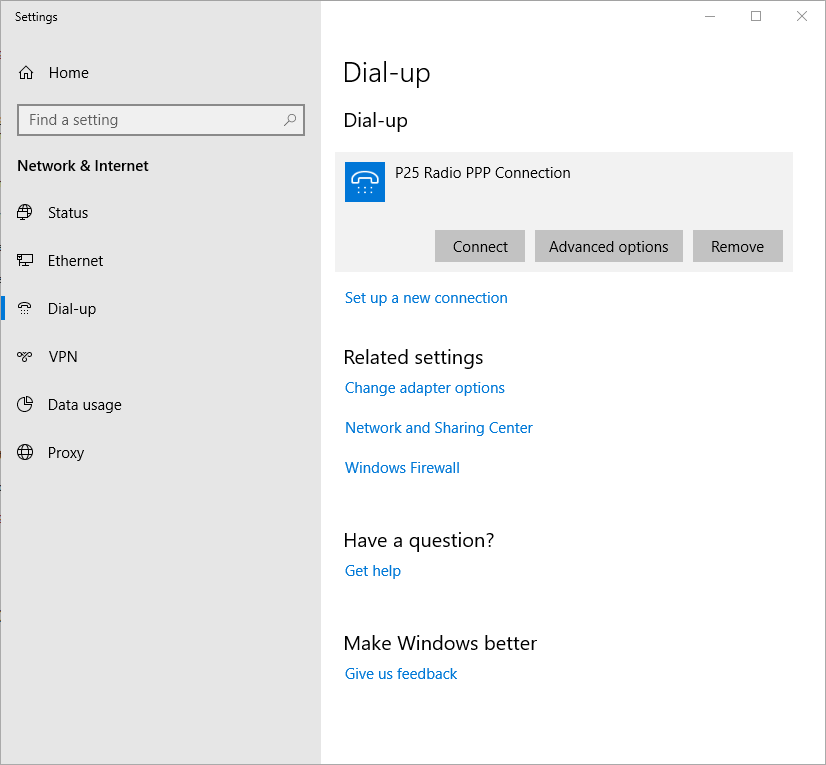
Click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection).



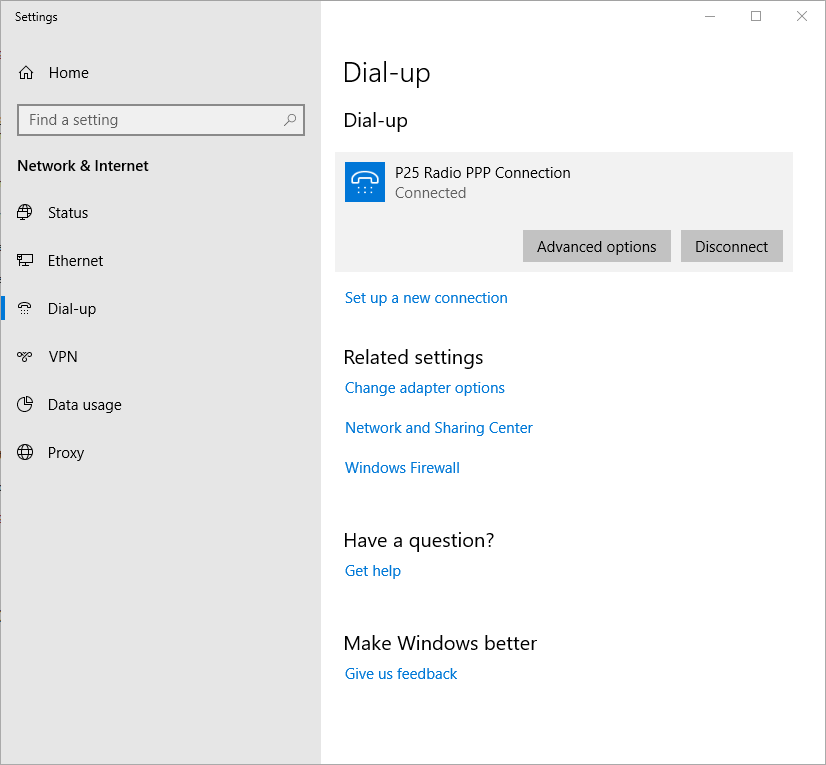
Click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection).



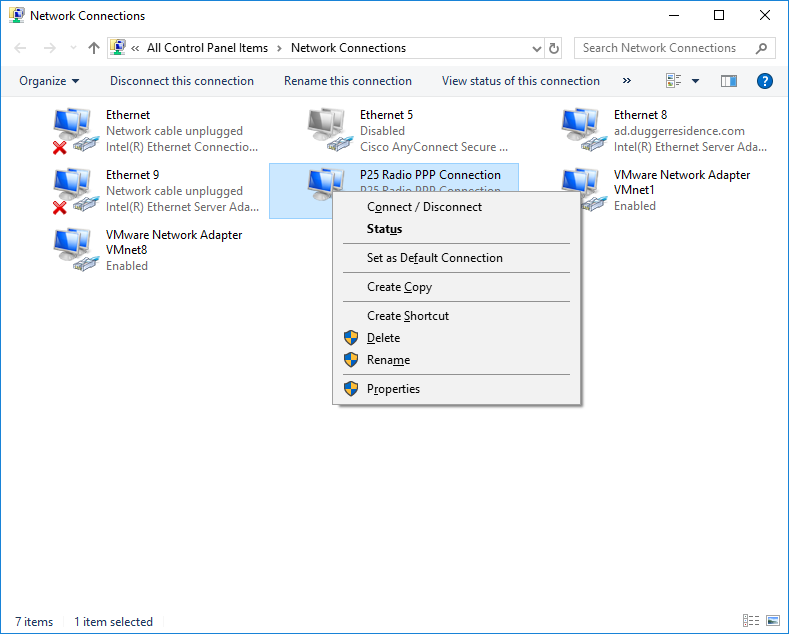
Click ‘Connect’.



Verify that the ‘P25 Radio Serial Modem’ (or whatever you named the dial-up connection) shows ‘Connected’.



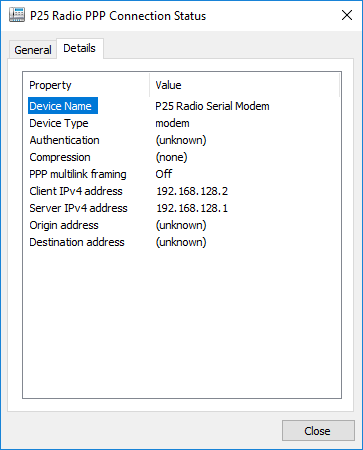
Right click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection), and click ‘Status.



Click ‘Details’.

The radio IP address is what appears in the ‘Server IPv4 address’ field.

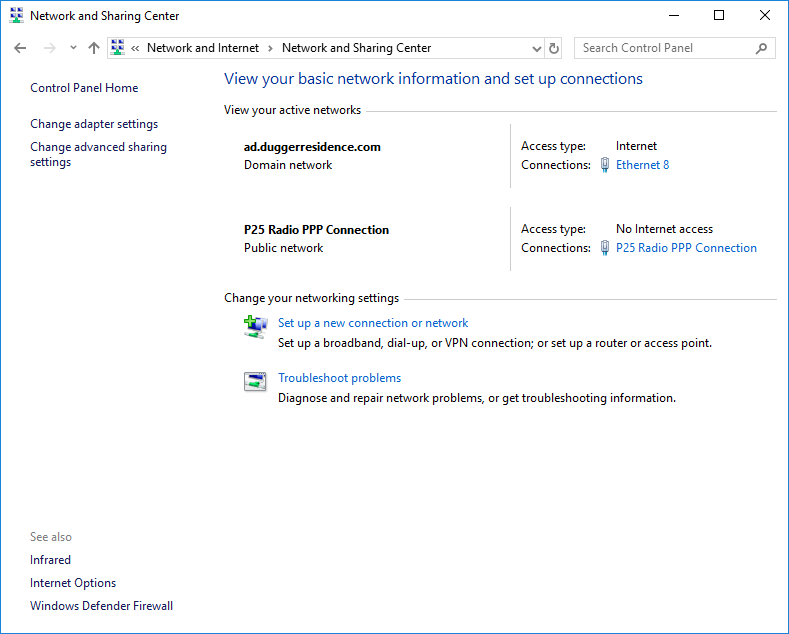
Click ‘Close’.



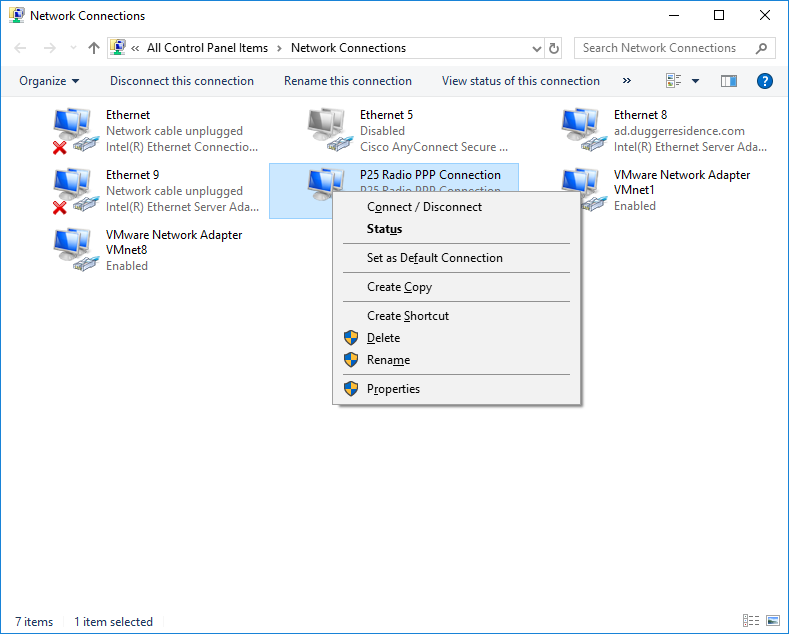
### Disconnection

Open the Network and Sharing Center.

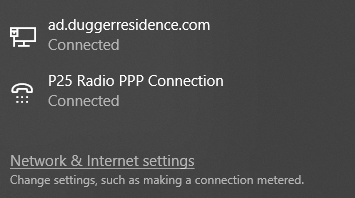
Click ‘Change Adapter Settings’.



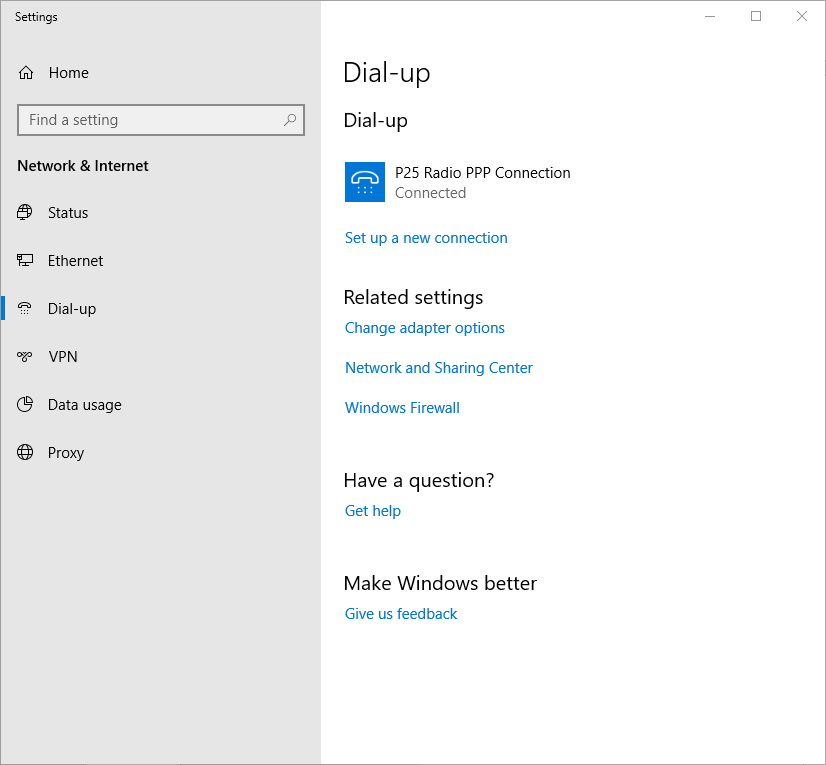
Right click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection), and click ‘Connect / Disconnect.



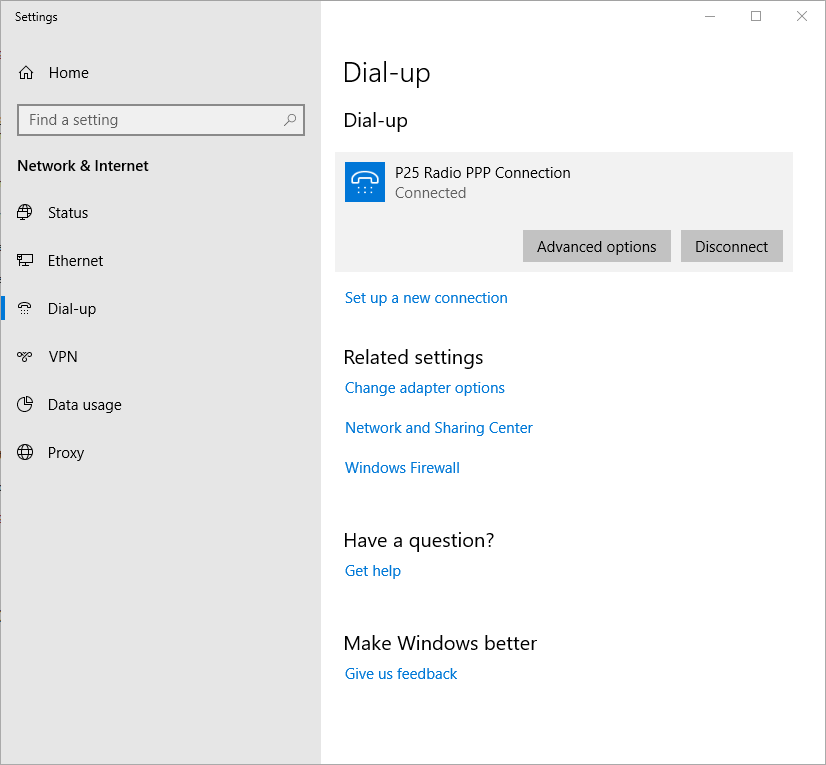
Click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection).



Click ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection).

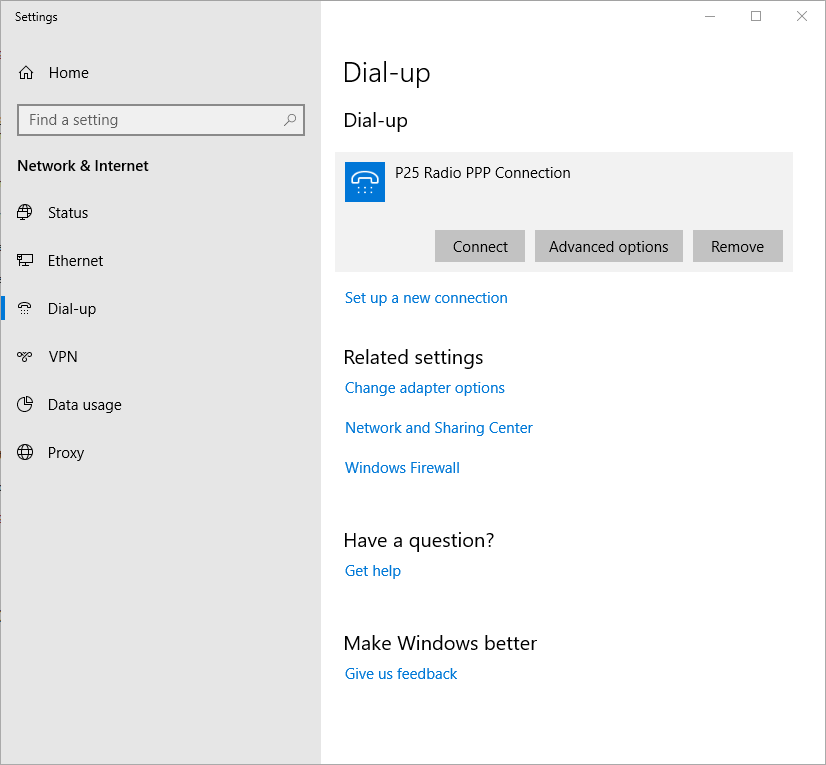


Click ‘Disconnect.



Verify that the ‘P25 Radio PPP Connection’ (or whatever you named the dial-up connection) does not show the ‘Connected’ status.

Disconnect the radio from the serial port.



# License

Copyright 2019 Daniel Dugger

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# Manual Revision History

|  |  |  |
| --- | --- | --- |
| **Revision #** | **Date** | **Description** |
| 1 | 2019-01-17 | Initial Release for 1.0.0.0 |