WaveShark Internet Gateway

User Manual

Document version 1.0.1
2023-01-18

Covers *WaveShark Communicator* firmware version 1.4.0 and above
Covers *WaveShark Internet Gateway* version 1.0.2 and above

Table of Contents

WaveShark Internet Gateway introduction....3
WaveShark Internet Gateway basic required connections....4
Creating Internet-interconnected WaveShark networks....5
Segregating traffic when sharing a common MQTT server....8
Running the WaveShark Internet Gateway software on Windows....9
Running the WaveShark Internet Gateway software on other platforms....11
Addressing the Gateway....12
Gateway announcements....13
WaveShark Internet Gateway end-to-end encryption....14
Encryption key and Initialization Vector recommendations....14
Non-private communications....14

WaveShark Internet Gateway introduction

The WaveShark Internet Gateway in its current form is a piece of software that allows WaveShark Communicator users to connect individual WaveShark networks together over end-to-end encrypted Internet links using publicly or privately hosted MQTT servers. It is currently available for download from the www.waveshark.net web site as a stand-alone .EXE program for Windows computers and also as Python source code upon request for running on Linux and other computers.

Future plans include making the WaveShark Internet Gateway available as an “appliance” (similar to a pre-packaged Wi-Fi router) so that end users do not have to deal with some of the more technical aspects of running this software on their computers.

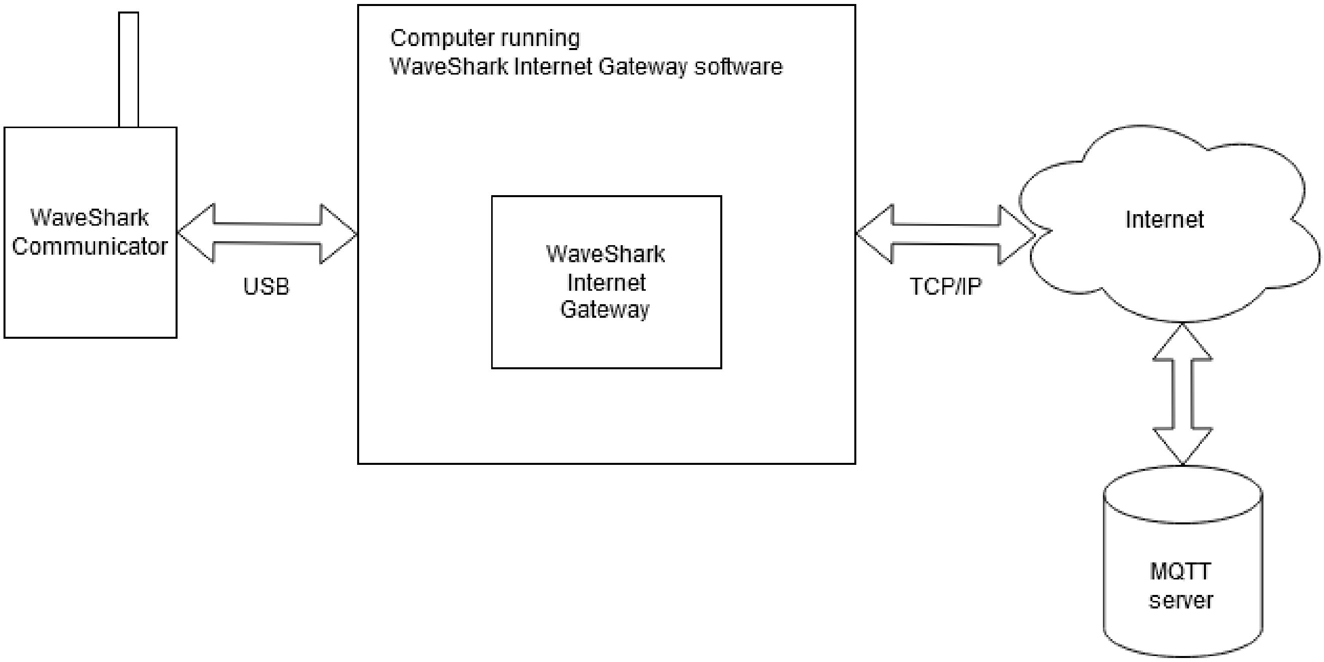
WaveShark Internet Gateway basic required connections

The WaveShark Internet Gateway generally requires a computer which is connected to the Internet and which has a WaveShark Communicator connected to it via USB.

Additionally, an Internet MQTT server is required. Thankfully, a free and publicly-hosted Internet MQTT server is available at ***broker.mqttdashboard.com***. This is the MQTT server that the WaveShark Internet Gateway will connect to by default. We believe that this is a reasonable option since all messages sent and received by the WaveShark Internet Gateway are encrypted and unable to be read by anyone without the correct encryption key. Additionally, only those who have the correct encryption key can introduce messages into the network.

An alternative MQTT server, including one which is privately hosted, can easily be used in place of this default option. A plethora of free MQTT server software is available on the Internet. One such piece of software that we have experience with is the ***Eclipse Mosquitto*** software, which is a free and open source MQTT message server available for download at ***www.mosquitto.org***.

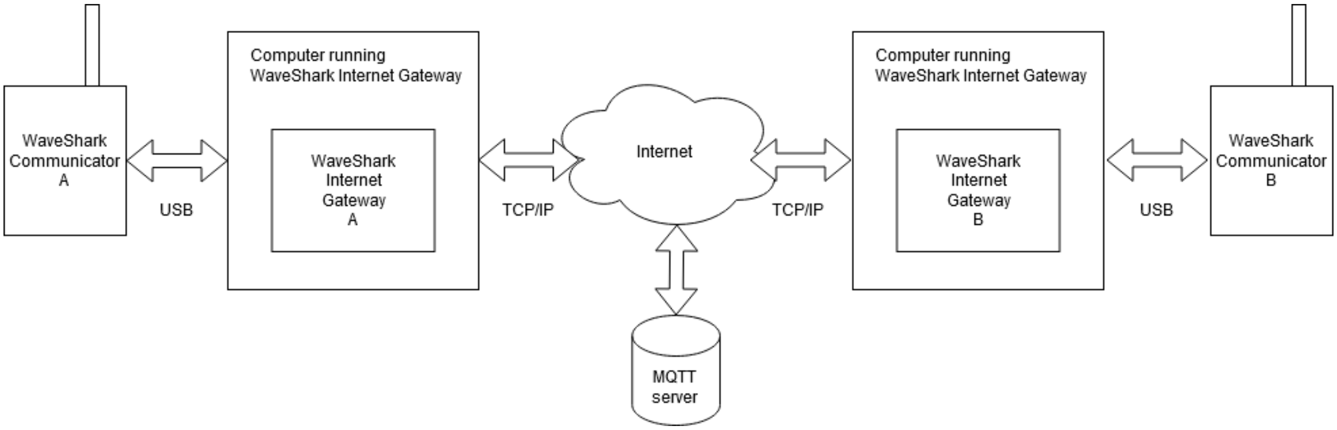
The diagram below shows the basic connections generally required of a computer running the WaveShark Internet Gateway software.



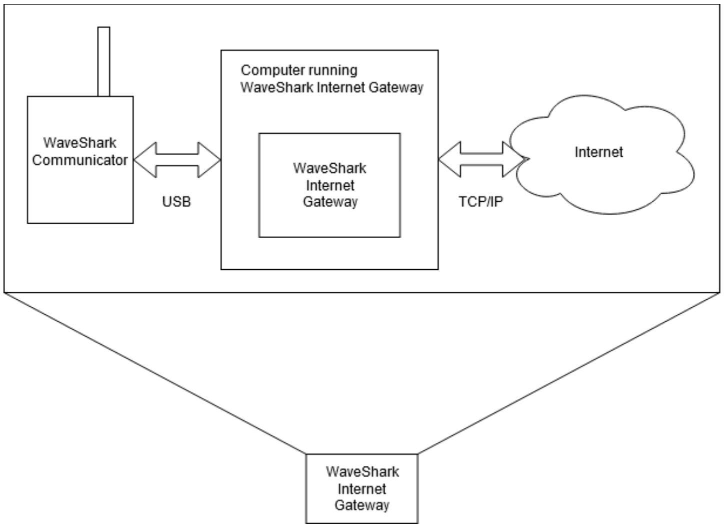
Creating Internet-interconnected WaveShark networks

Two or more computers running the WaveShark Internet Gateway software can be used to bridge together two or more geographically distant WaveShark networks.

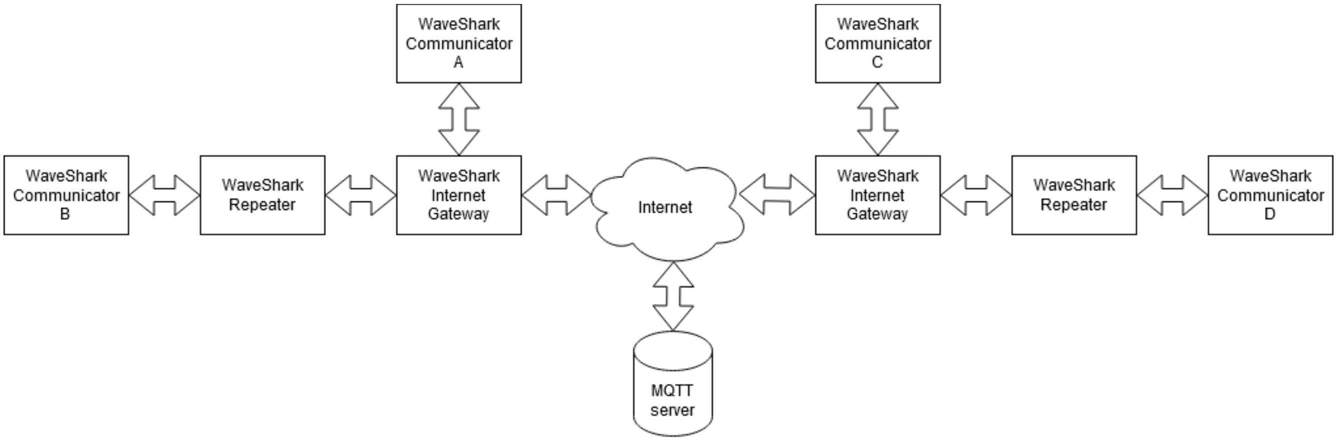
The diagram below shows two WaveShark Internet Gateways operating with the same encryption key and the same *message topic* (more on *message topics* later). Whether WaveShark Communicators A and B are located on either ends of a large city, a state, a country, or even the world, any message received by WaveShark Communicator A can be forwarded to all WaveShark devices within range of WaveShark Communicator B and vice versa. In this way, a network of WaveShark devices centered around WaveShark Communicator A could all be in contact with a network of WaveShark devices centered around WaveShark Communicator B.


WaveShark Communicator A
USB
Computer running WaveShark Internet Gateway
WaveShark Internet Gateway A
TCP/IP
Internet
TCP/IP
Computer running WaveShark Internet Gateway
WaveShark Internet Gateway B
USB
WaveShark Communicator B
MQTT server

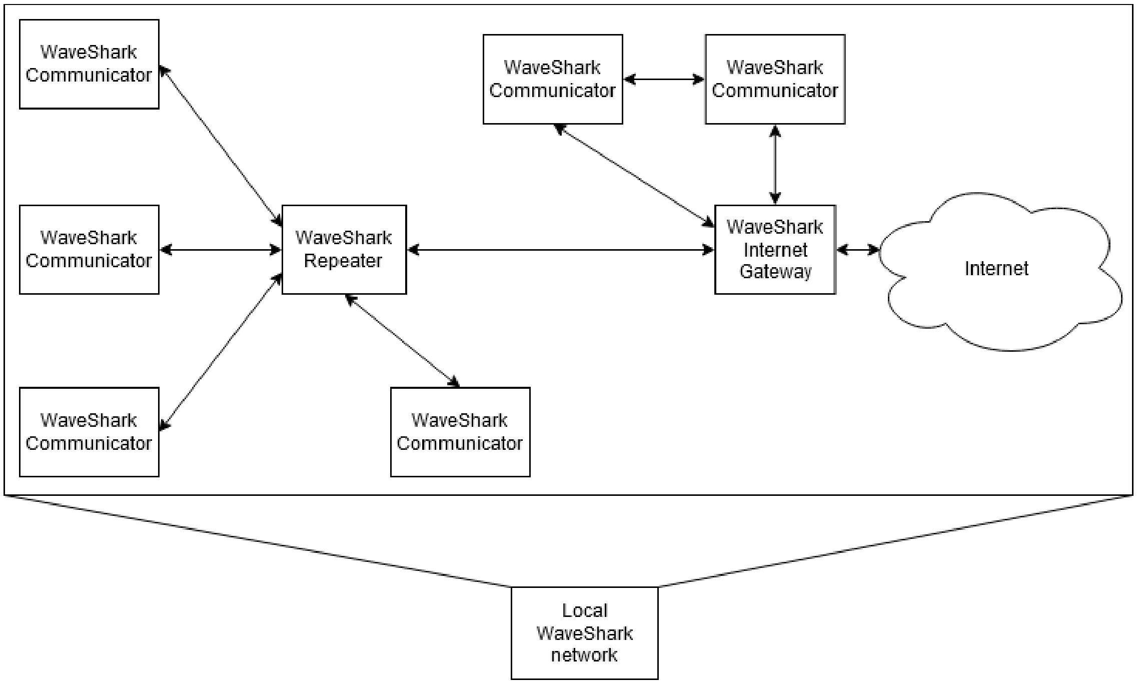
The WaveShark Internet Gateway software running on a computer connected to the Internet and connected to a WaveShark Communicator via USB will be condensed into the following icon in all subsequent diagrams in order to condense the size of said diagrams and to allow us to explore bigger ideas:


WaveShark Communicator
USB
Computer running WaveShark Internet Gateway
WaveShark Internet Gateway
TCP/IP
Internet
WaveShark Internet Gateway

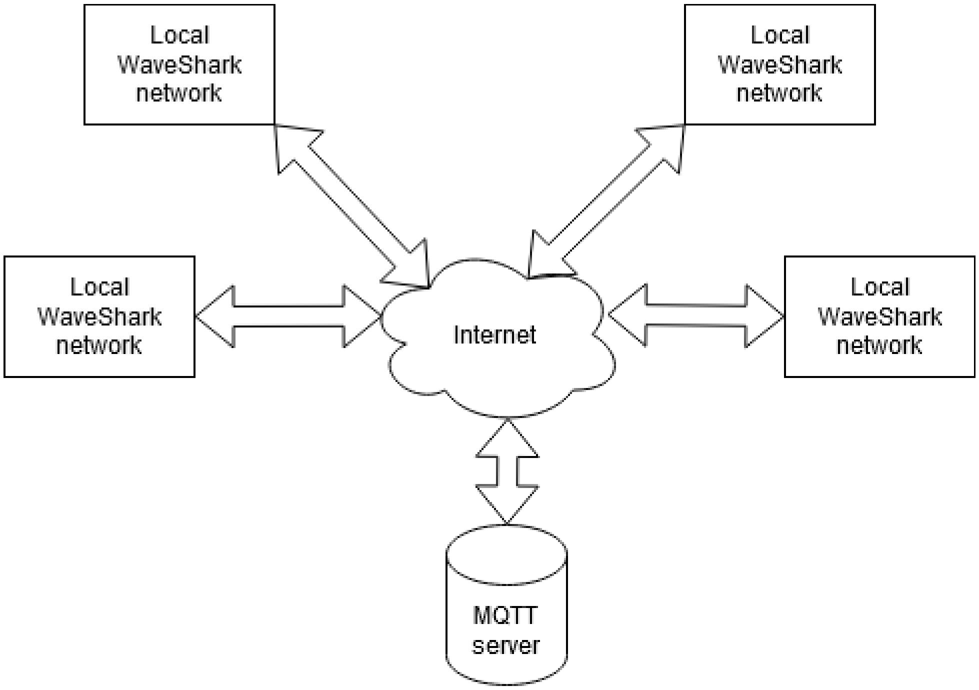
The diagram below shows two local WaveShark networks interconnected via WaveShark Internet Gateways. Each example network is shown with a WaveShark Communicator within range of the Gateway, a WaveShark Repeater within range of the Gateway, and a distant WaveShark Communicator that reaches the Gateway via the Repeater. All four WaveShark Communicators (A, B, C, D) are able to communicate with one another. Much more complex arrangements are entirely feasible. Also, any number of Gateways can be interconnected.



A WaveShark Internet Gateway in range of a number of WaveShark Communicator and WaveShark Repeater devices (a local WaveShark network with an Internet Gateway) will be condensed into the following icon in all subsequent diagrams in order to condense the size of said diagrams and to allow us to explore bigger ideas:



The diagram below shows a handful of local WaveShark networks interconnected via WaveShark Internet Gateways:

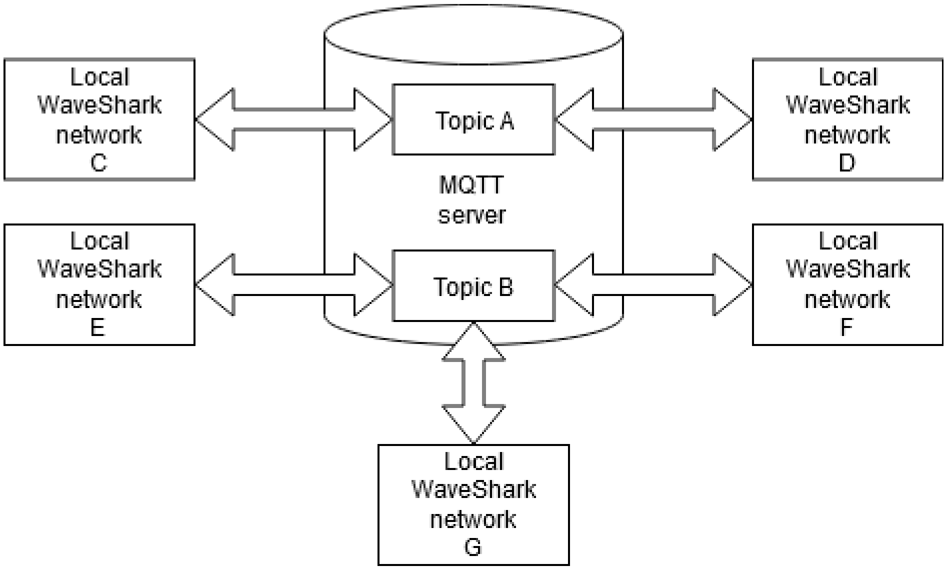


Segregating traffic when sharing a common MQTT server

Traffic from various WaveShark Internet Gateways sharing a common MQTT server can be segregated by using different *message topics*.

The diagram below shows a handful of local WaveShark networks sharing a common MQTT server but keeping one set of local WaveShark networks separate from another set of local WaveShark networks so that not every local WaveShark network sees the traffic from all other local WaveShark networks.

In this diagram, traffic between networks C and D are connected and traffic between networks E, F, and G are connected.


Local WaveShark network C
Topic A
Local WaveShark network D
MQTT server
Local WaveShark network E
Topic B
Local WaveShark network F
Local WaveShark network G

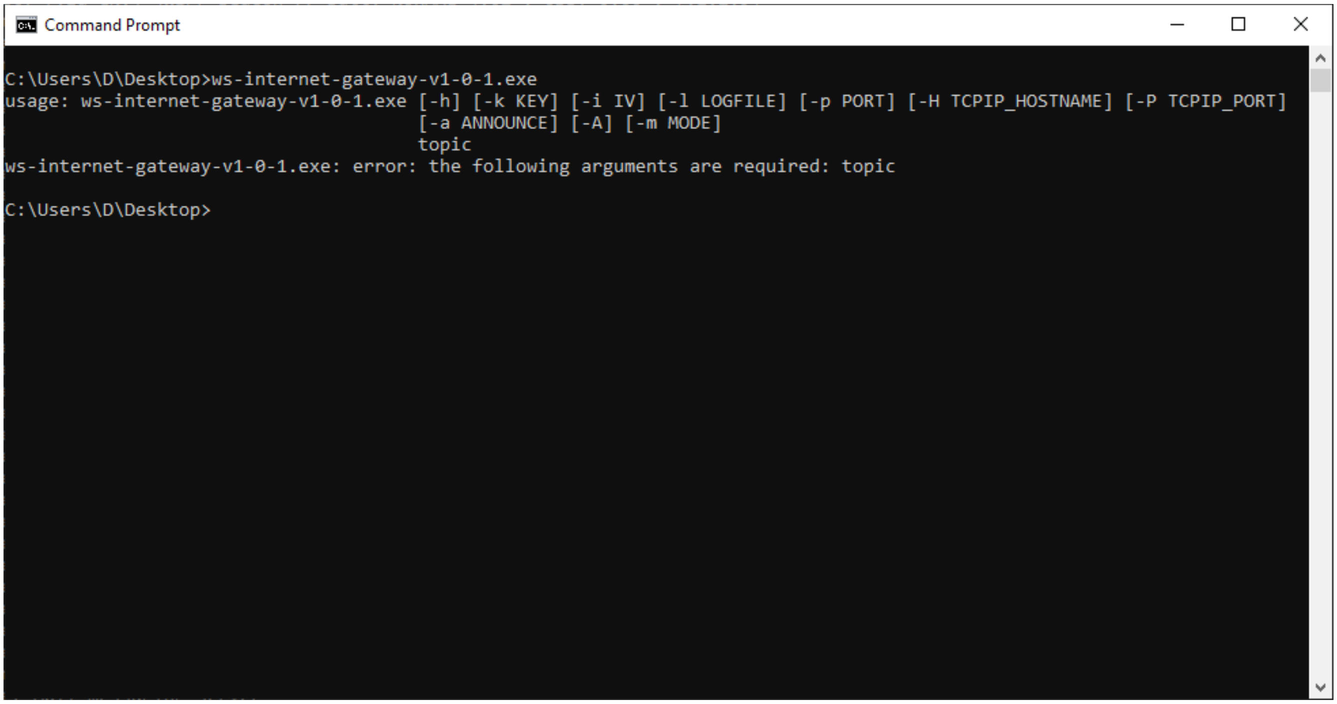
Running the WaveShark Internet Gateway software on Windows

Download the latest version of the WaveShark Internet Gateway software for Windows from the WaveShark web site, www.waveshark.net. It is available under the *Downloads* section of the web site.

The WaveShark Internet Gateway software for Windows is provided as a signed stand-alone executable (.EXE) and does not require installation. Simply move or copy the downloaded .EXE file to the directory (folder) that you would like to run the program from.

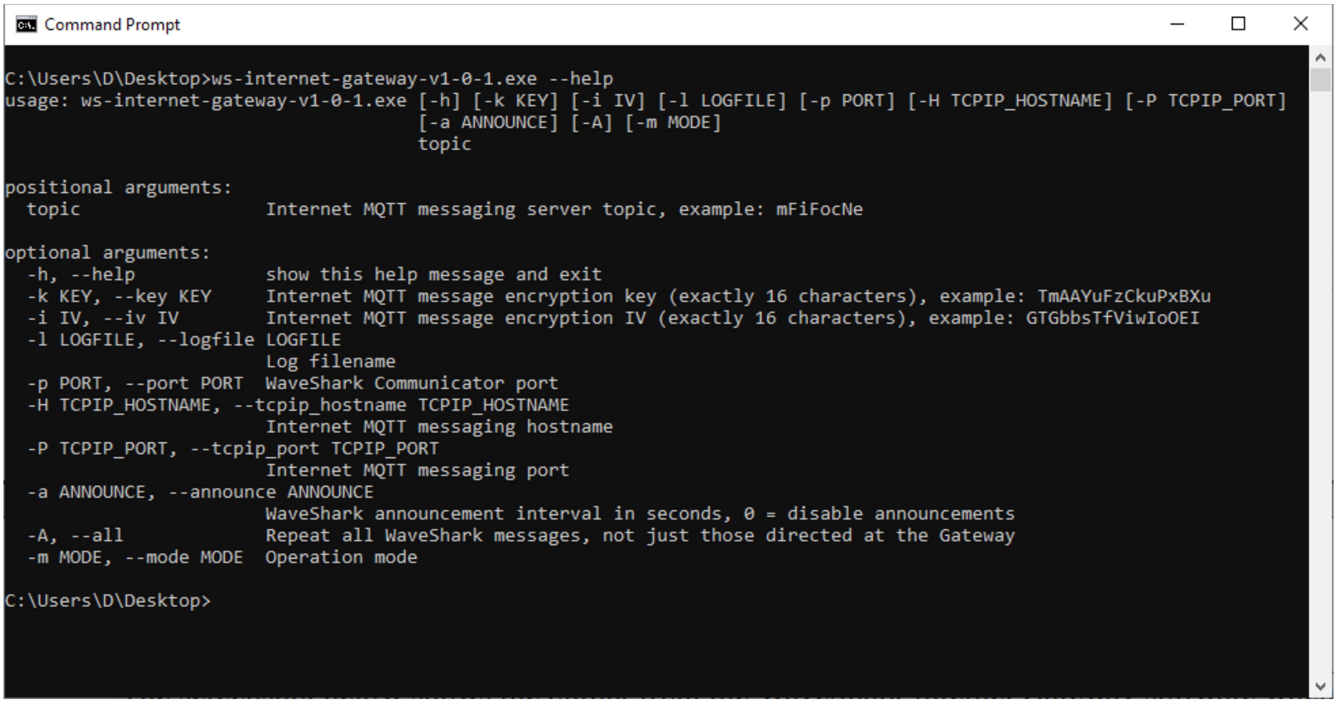
It is recommended that you run the program from a Windows Command Prompt instead of simply double-clicking on the program from Windows Explorer. This is so that you can see any output from the program before the window simply closes on you.

The screenshot below shows the output from the WaveShark Internet Gateway software when run without any command-line arguments:



```
C:\Users\D\Desktop>ws-internet-gateway-v1-0-1.exe
usage: ws-internet-gateway-v1-0-1.exe [-h] [-k KEY] [-i IV] [-l LOGFILE] [-p PORT] [-H TCPIP_HOSTNAME] [-P TCPIP_PORT]
                                      [-a ANNOUNCE] [-A] [-m MODE]
                                      topic
ws-internet-gateway-v1-0-1.exe: error: the following arguments are required: topic

C:\Users\D\Desktop>
```

The screenshot below shows the output from the WaveShark Internet Gateway software when run with the *-h* or *–help* arguments in order to display its basic help information:



```
C:\Users\D\Desktop>ws-internet-gateway-v1-0-1.exe --help
usage: ws-internet-gateway-v1-0-1.exe [-h] [-k KEY] [-i IV] [-l LOGFILE] [-p PORT] [-H TCPIP_HOSTNAME] [-P TCPIP_PORT]
                                      [-a ANNOUNCE] [-A] [-m MODE]
                                      topic

positional arguments:
  topic                 Internet MQTT messaging server topic, example: mFiFocNe

optional arguments:
  -h, --help            show this help message and exit
  -k KEY, --key KEY     Internet MQTT message encryption key (exactly 16 characters), example: TmAAYuFzCkuPxBXu
  -i IV, --iv IV        Internet MQTT message encryption IV (exactly 16 characters), example: GTGbbsTfViwIoOEI
  -l LOGFILE, --logfile LOGFILE
                        Log filename
  -p PORT, --port PORT  WaveShark Communicator port
  -H TCPIP_HOSTNAME, --tcpip_hostname TCPIP_HOSTNAME
                        Internet MQTT messaging hostname
  -P TCPIP_PORT, --tcpip_port TCPIP_PORT
                        Internet MQTT messaging port
  -a ANNOUNCE, --announce ANNOUNCE
                        WaveShark announcement interval in seconds, 0 = disable announcements
  -A, --all             Repeat all WaveShark messages, not just those directed at the Gateway
  -m MODE, --mode MODE  Operation mode

C:\Users\D\Desktop>
```

A *messaging topic* must always be provided to the WaveShark Internet Gateway software. In fact, this is the only single piece of information which is required to run the software. All other arguments to the software are strictly optional.

We will now cover all options available in the software, one by one.

- -h or –help: Display basic help information
- -k or --key: Specify the encryption key to use. The encryption key must be exactly 16 characters long. If an encryption key is not specified then all messages will be encrypted with a simple default encryption key.
- -i or –iv: Specify the encryption Initialization Vector (IV) to use. The encryption IV must be exactly 16 characters long. If an encryption IV is not specified then all messages will be encrypted with a simple default encryption IV. More information on encryption Initialization Vectors is available from sources such as *Wikipedia*, *Stack Overflow*, and many others.
- -l or –logfile: Write all output to a log file, in addition to the console window. If the file specified does not already exist then it will be created. If the file already exists then it will be appended to.
- -p or –port: Specify the COM port which your WaveShark Communicator is attached to. If the port is not specified then the software will automatically connect to a WaveShark Communicator if one and only one is available to connect to. If more than one WaveShark Communicator is available to connect to then the port must be specified.

- -H or –tcpip_hostname: Specify the hostname or IP address of the Internet TCP/IP MQTT server to use for message passing. If the hostname is not specified then the software will automatically default to using the publicly available ***broker.mqttdashboard.com*** server.
- -P or –tcpip_port: Specify the port of the Internet TCP/IP MQTT server to use for message passing. If the port is not specified then the software will automatically default to the typical MQTT TCP/IP port ***1883***.
- -a or –announce: Specify the number of seconds between each *announcement* that the WaveShark Internet Gateway sends to nearby WaveShark devices. Use 0 to disable the sending of announcements. If an announcement interval is not specified then the software will automatically default to sending an announcement every 600 seconds, or every 10 minutes. More on *announcements* later.
- -A or –all: Use this argument to forward ***all*** local WaveShark traffic to the Internet, not just traffic addressed to the Gateway. By default, only traffic specifically addressed to the Gateway will be forwarded to the Internet. More on *addressing the Gateway* later.
- -m or –mode: Specify the *operation mode*. By default, the WaveShark Internet Gatway software requires that a WaveShark Communicator be connected to the computer running the Gateway software and that Gateway will forward local WaveShark traffic to the Internet and traffic from the Internet to the local WaveShark network. This is referred to as *normal operation mode*. Alternatively, the Gateway can operate in *Internet MQTT listener mode* by using the -m 2 or –mode 2 argument. In this mode, it is not required that a WaveShark Communicator be connected to the computer running the Gateway software. *Internet MQTT listener mode* will simply connect to the specified MQTT server and listen to Internet messages, displaying them on the console and optionally writing them to a log file. It might be helpful to think of this mode as a *tap*. We believe that there will be many creative uses of this operating mode. Of course, no one can "tap into" any messaging stream unless they have the correct encryption key and encryption Initialization Vector.

Running the WaveShark Internet Gateway software on other platforms

The WaveShark Internet Gateway software for Windows is provided as a signed stand-alone .EXE program. Behind the scenes, the Gateway software is written in Python and *pyinstaller* is used to build a stand-alone .EXE program which does not require end users to have any knowledge of Python, *pip*, Python *virtual environments*, etc. By request, the Python source code can be made available to anyone wishing to run the WaveShark Internet Gateway software on platforms such as Linux, macOS, etc. The WaveShark Internet Gateway software has been tested on Linux and should run on just about any Linux installation without any modifications.

Contact us at info@waveshark.net for more information on running the WaveShark Internet Gateway on platforms other than Windows.

Addressing the Gateway

When the WaveShark Internet Gateway is operating in its default mode, it will only forward WaveShark messages that are specifically addressed to it. The -A or –all option can be used to forward all WaveShark messages, not just those which are addressed to the Gateway.

To address a message to the Gateway for forwarding, write a WaveShark message which starts with the name of the Gateway, followed by SEND, followed by the message you would like to send.

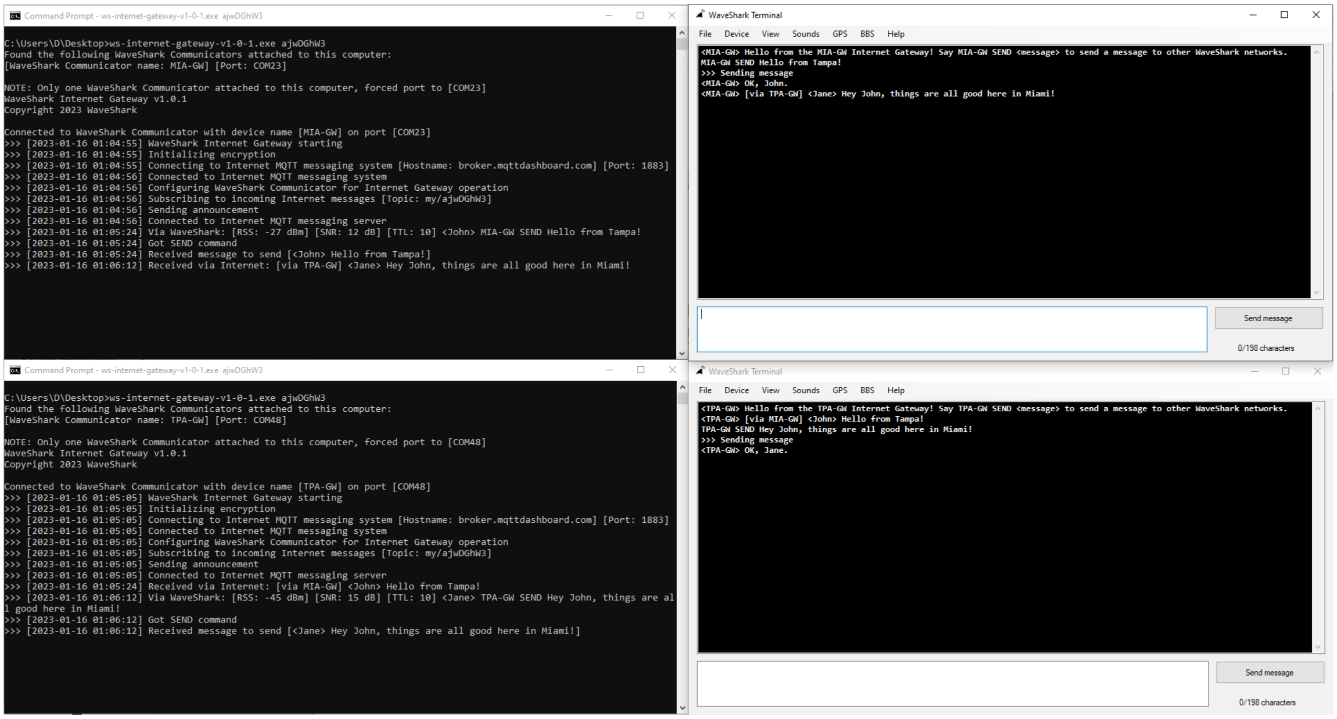
For example:

```
TPA-GW SEND This is a message from Tampa.
```

```
MIA-GW SEND Is anyone in Tampa on-line right now?
```

By default, the WaveShark Internet Gateway will send *announcements* (more on *announcements* below) to its local WaveShark network reminding users that the Gateway is there and providing instructions on how to address messages to the Gateway.

The screenshot below shows two WaveShark Internet Gateways running and two WaveShark users interacting with one another via their local Gateways. The screenshot also shows the announcement messages from each Gateway:



```
C:\Users\D\Desktop>ws-internet-gateway-v1-0-1.exe ajwDGhW3
Found the following WaveShark Communicators attached to this computer:
[WaveShark Communicator name: MIA-GW] [Port: COM23]

NOTE: Only one WaveShark Communicator attached to this computer, forced port to [COM23]
WaveShark Internet Gateway v1.0.1
Copyright 2023 WaveShark

Connected to WaveShark Communicator with device name [MIA-GW] on port [COM23]
>>> [2023-01-16 01:04:55] WaveShark Internet Gateway starting
>>> [2023-01-16 01:04:55] Initializing encryption
>>> [2023-01-16 01:04:55] Connecting to Internet MQTT messaging system [Hostname: broker.mqttdashboard.com] [Port: 1883]
>>> [2023-01-16 01:04:56] Connected to Internet MQTT messaging system
>>> [2023-01-16 01:04:56] Configuring WaveShark Communicator for Internet Gateway operation
>>> [2023-01-16 01:04:56] Subscribing to incoming Internet messages [Topic: my/ajwDGhW3]
>>> [2023-01-16 01:04:56] Sending announcement
>>> [2023-01-16 01:04:56] Connected to Internet MQTT messaging server
>>> [2023-01-16 01:05:24] Via WaveShark: [RSS: -27 dBm] [SNR: 12 dB] [TTL: 10] <John> MIA-GW SEND Hello from Tampa!
>>> [2023-01-16 01:05:24] Got SEND command
>>> [2023-01-16 01:05:24] Received message to send [<John> Hello from Tampa!]
>>> [2023-01-16 01:06:12] Received via Internet: [via TPA-GW] <Jane> Hey John, things are all good here in Miami!
```

```
<MIA-GW> Hello from the MIA-GW Internet Gateway! Say MIA-GW SEND <message> to send a message to other WaveShark networks.
MIA-GW SEND Hello from Tampa!
>>> Sending message
<MIA-GW> OK, John.
<MIA-GW> [via TPA-GW] <Jane> Hey John, things are all good here in Miami!
```

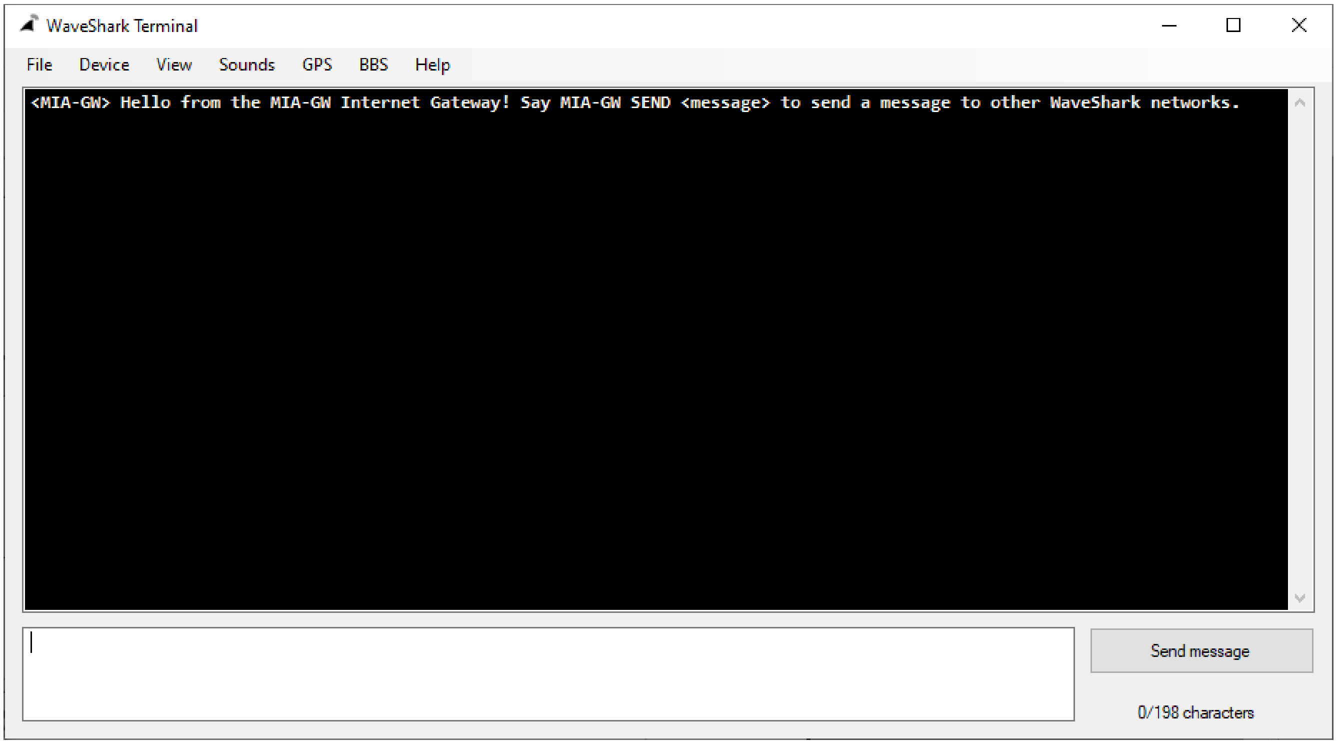
```
C:\Users\D\Desktop>ws-internet-gateway-v1-0-1.exe ajwDGhW3
Found the following WaveShark Communicators attached to this computer:
[WaveShark Communicator name: TPA-GW] [Port: COM48]

NOTE: Only one WaveShark Communicator attached to this computer, forced port to [COM48]
WaveShark Internet Gateway v1.0.1
Copyright 2023 WaveShark

Connected to WaveShark Communicator with device name [TPA-GW] on port [COM48]
>>> [2023-01-16 01:05:05] WaveShark Internet Gateway starting
>>> [2023-01-16 01:05:05] Initializing encryption
>>> [2023-01-16 01:05:05] Connecting to Internet MQTT messaging system [Hostname: broker.mqttdashboard.com] [Port: 1883]
>>> [2023-01-16 01:05:05] Connected to Internet MQTT messaging system
>>> [2023-01-16 01:05:05] Configuring WaveShark Communicator for Internet Gateway operation
>>> [2023-01-16 01:05:05] Subscribing to incoming Internet messages [Topic: my/ajwDGhW3]
>>> [2023-01-16 01:05:05] Sending announcement
>>> [2023-01-16 01:05:05] Connected to Internet MQTT messaging server
>>> [2023-01-16 01:05:24] Received via Internet: [via MIA-GW] <John> Hello from Tampa!
>>> [2023-01-16 01:06:12] Via WaveShark: [RSS: -45 dBm] [SNR: 15 dB] [TTL: 10] <Jane> TPA-GW SEND Hey John, things are al
l good here in Miami!
>>> [2023-01-16 01:06:12] Got SEND command
>>> [2023-01-16 01:06:12] Received message to send [<Jane> Hey John, things are all good here in Miami!]
```

```
<TPA-GW> Hello from the TPA-GW Internet Gateway! Say TPA-GW SEND <message> to send a message to other WaveShark networks.
<TPA-GW> [via MIA-GW] <John> Hello from Tampa!
TPA-GW SEND Hey John, things are all good here in Miami!
>>> Sending message
<TPA-GW> OK, Jane.
```

Gateway announcements

By default, the WaveShark Internet Gateway will send an announcement every 600 seconds (every 10 minutes) announcing its presence and telling local WaveShark users how to address the Gateway. Announcements can be disabled by using the -a 0 or –all 0 argument. The announcement interval can be changed by specifying the desired number of seconds to the -a or –all argument.

The screenshot below shows a WaveShark Internet Gateway sending its announcement to its local WaveShark users:



```
<MIA-GW> Hello from the MIA-GW Internet Gateway! Say MIA-GW SEND <message> to send a message to other WaveShark networks.
```

WaveShark Internet Gateway end-to-end encryption

All messages originating from the WaveShark Internet Gateway software are encrypted using AES encryption before being transmitted via the Internet to the MQTT message store. Therefore, all messages that travel over the Internet are encrypted and additionally all messages stored in the MQTT message store are encrypted. Likewise, all messages received via the Internet from the MQTT message store are encrypted. Only the WaveShark Internet Gateways hold the necessary encryption keys to recover these messages.

Also, no messages can be introduced into the WaveShark Internet Gateways or related MQTT message stores unless the sender holds the necessary encryption keys to properly encrypt the messages before sending them. The WaveShark Internet Gateway software will automatically reject any message which has not first been properly encrypted with the correct encryption keys.

In addition, all WaveShark devices (WaveShark Communicators and WaveShark Repeaters) feature built-in optional AES encryption. Enabling encryption in the WaveShark Internet Gateway and on all related WaveShark devices means having complete end-to-end encryption.

Encryption key and Initialization Vector recommendations

It is highly likely that all necessary message privacy can be achieved by simply using a random 16 character string for the encryption key and another random 16 character string for the encryption Initialization Vector (IV).

For example:

- `Encryption key: 3JwdHUZc8AzgsBzH, encryption IV: Co5zZ0trr1Zv0W8k`
- `Encryption key: eYO36e25IS0UXw4I, encryption IV: ncB6FQxIclc99Nl4`
- `Encryption key: QkkB7cZAa7flR7wE, encryption IV: Ns9Dem0bdwGWbNoK`

DO NOT ACTUALLY USE ANY OF THE ABOVE KEYS OR INITIALIZATION VECTORS. THESE ARE SIMPLY PROVIDED AS EXAMPLES OF WHAT YOUR KEYS MIGHT LOOK LIKE.

Non-private communications

It might not always be the case that you want to keep communications private. There very well may be cases where you would like any interested party to be able to join in. In this case, simply do not specify an encryption key or encryption Initialization Vector. Technically speaking, any WaveShark Internet Gateway operating without specified encryption keys will still encrypt its messages, but all Gateways will be using the same encryption key and encryption IV and thus will have the effect of anyone operating a Gateway without specifying this information will be able to join in on the message traffic.

By default, the WaveShark Internet Gateway will use the following values for the encryption key and encryption Initialization Vector, respectively:

- `aaaaaaaaaaaaaaaa`

- bbbbbbbbbbbbbbbb