EtherHaul

SW Upgrade Procedure

Dec 2013

SIKLU
43 Hasivim St., Kiriat Matalon
Petach Tikva 49517
Phone: +972 3 921 4015 Fax: +972 3 921 4162 **www.siklu.com**

Table of Contents

1. Purpose

The purpose of this document is to describe Siklu's recommended SW upgrade procedure for its **EtherHaul** family radio links, loaded with SW release 2.0.0.x or higher.

EtherHaul SW download requires FTP server. The EtherHaul ODU's internal FTP client will access the external FTP server that will host the SW version file.

Any FTP server software available on the web can be used for SW download.

Appendix A of this document describes the SW download procedure using one of the available freeware FTP servers.

Alternatively, TFTP server can be used as well.

2. SW Upgrade Overview

This document describes the SW upgrade steps, covering:

1. Checking current SW versions
2. Recording the current ODU configuration
3. SW download and upgrade
4. Acceptance tests after upgrade
5. (Appendix) FTP Server installation, configuration and launch

Note:

FTP service must be free and not blocked by Firewall/Antivirus or occupied by other software or services.

If you run into problems using the FTP SW upgrade, try using TFTP (often not blocked or used by other software services).

3. Checking Current SW Versions

Use the CLI or Web-GUI to check the current SW versions of the ODU.

Two SW banks available in the ODU:

6. Active version (Running status = Yes)
7. Offline or Standby version (Running status = No)

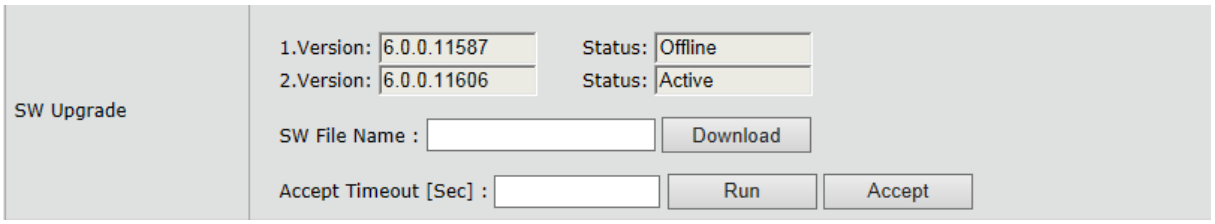
Downloaded SW replaces the Offline (Standby) version.

CLI:

```
ETH-1200> show sw

Flash Bank    Version                              Running      Scheduled to run
1             6.0.0.11606 2012-06-11 15:58:13      yes          no
2             6.0.0.11587 2012-03-20 14:59:57      no           no
```

Release info: Major Minor Sub Build #

Web-GUI (System->Maintenance):



4. Recording Current ODU Configuration

Use the CLI or Web-GUI to check the current ODU configuration.

Recording the ODU configuration prior to the SW upgrade will allow you to check and compare the ODU configuration after upgrade.

CLI:

1. Copy the current configuration of both Local and Remote ODUs to display (CLI screen)

   copy running-configuration display

2. Copy the configuration commands to a text file and save it.

Web-GUI:

1. Run script 'system_info' and save the output to a text file.

   System->Maintenance->Scripts->system_info->run

   The configuration commands are part of the output of the 'system_info' script.

5. SW Download and Upgrade

Use Siklu's CLI or Web-GUI to configure the SW download to the ODU after launching the FTP server.

You will receive the SW version file from Siklu.

The SW version file should be stored in the home path directory of the FTP server (for example: C:/publicftp).

Before starting the SW download, launch the FTP server and confirm it is running.

5.1 SW Download – Using CLI

1. Connect to the ODU using ssh client. You can use a common, open source SSH client programs such as PuTTY (can be downloaded from http://www.putty.org/).

- Login as user admin.
- Enter the password admin.

2. Use CLI to download and accept sw to the ODU using the copy sw command:

   copy sw ftp://<username>:<password>@<Server IP Address>/<sw image name>

For example:

FTP server IP 192.168.0.200, User=ftp, Password=admin, SW image sw-uimage-6.0.0.6343

```
ETH-1200> copy sw ftp://ftp:admin@192.168.0.200/sw-uimage-6.0.0.6343
Done
.....
finished
```

5.2 SW Upgrade – Using CLI

1. To activate the new downloaded sw (with 600 seconds timeout to accept it):

```
ETH-1200> run sw immediate 600
…….
```

The ODU will reboot (disconnecting the CLI session) and come up with the new downloaded sw with 'Running Status = wait to accept.

2. Reconnect using CLI and make sure the link is up. Refer to the 'Acceptance Tests after SW Upgrade' in the next session.

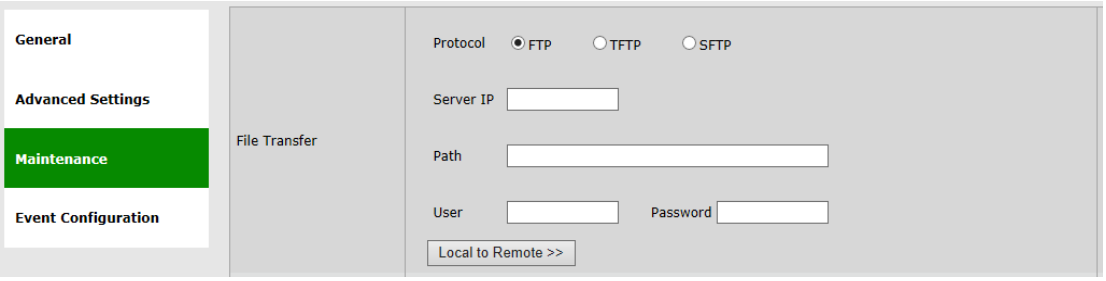
3. After you verify the new SW version is running as expected make sure to accept the new SW before the timeout expires:

```
ETH-1200> accept sw
```

5.3 SW Download and Upgrade – Using Web-GUI

1. Launch an Internet browser and enter the ODU's IP address in the address bar. For the default IP address enter: https://192.168.0.1.
2. Enter the username and password (default read/write access: user admin, password admin).

3. Go to System->Maintenance->File Transfer to configure the File Transfer attributes.



The administration of the file system is controlled by the File Transfer session. It includes the configuration files, SW version, licenses, scripts, inventory and more.

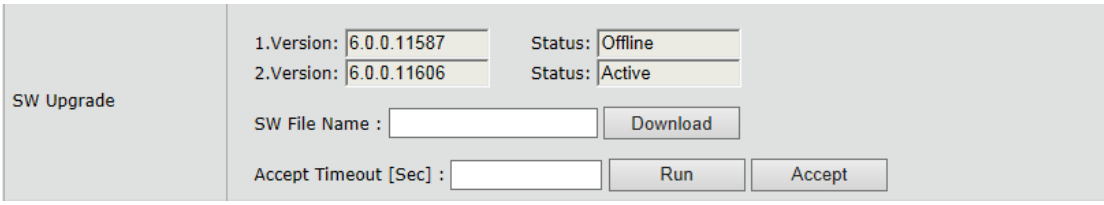
An external FTP, TFTP or SFTP server is required for file transfer.

In order to transfer files, FTP/TFTP/SFTP server must be running and the file transfer attributes must be configured.

This section allows configuring the following parameters:

- Protocol – FTP, TFTP or SFTP.
- Server IP – the IP address of the server where the FTP/TFTP/SFTP server is running on.
- Path – the path of the stored file (or target destination) relative to the directory used for file transfers as configured in the server. If left blank, file transfer will be from/to the server's Root (or Home) directory.
- User – user name, as defined in the server. Leave blank if anonymous user defined.
- Password – password, as defined in the server. Leave blank if anonymous user defined.

4. Go to System->Maintenance->SW Upgrade to download and upgrade the SW.



This section allows configuring the following parameters:

- SW File Name – The name of the software file to download.
- Accept Timeout [Sec] – time out in seconds in which the new software should be accepted. If the new software is not accepted within the timeout period, the system will

reset and rollback to the previously active software. It is recommended to use 600 seconds timeout whenever upgrading a software.

Click **Download** to start the software download from the server to the system.

Click **Upgrade** to activate the downloaded software. This action will result in system reset.

Click **Accept** to accept the new SW.

5.4 Notes regarding Upgrade Steps

When upgrading a working link with management access from one side (Local end), follow these steps in order to avoid losing management to Remote end):

1. Download the new SW to both Local and Remote ODUs.
2. Save current configuration on both Local and Remote ODUs
   copy running-configuration startup-configuration
3. Activate the downloaded SW on the Remote ODU with 600 seconds timeout
   run sw immediate 600
4. Activate the downloaded SW on the Local ODU with 600 seconds timeout
   run sw immediate 600
5. Wait for the ODUs to complete reboot (~2 minutes) and verify the link is up with management connection to Remote ODU
6. Accept the new SW on the Remote ODU
   accept sw
7. Accept the new SW on the Local ODU
   accept sw

6. Acceptance Tests after SW Upgrade

After upgrading to a new SW, it is recommended to following acceptance tests to make sure radio link is restored correctly and new SW functions properly.

1. RF Link verification

The purpose of this test is to verify the RF link status as before the upgrade.

- Link is up
- RSSI (Receive Signal Strength Indication) is similar to the RSSI value recorded prior to the upgrade
- CINR (Carrier to Interference + Noise Ratio) is similar to the CINR value recorded prior to the upgrade
- ODU reaches to the modulation it had prior to the upgrade

2. RF Link Test

The purpose of this test is to verify error-free operation of the radio link by checking the RF Statistics counters for lost/errored packets.

- No errors/loss on the RF Statistics counters.

3. Ethernet Services Test

The purpose of this test is to verify correct Ethernet services flow and error-free operation.

- Connect the radio link to end-equipment on site and verify proper and packet-loss-free traffic over the link.

4. Management Verification

The purpose of this test is to verify proper management of the link.

Verify correct management/CLI connection to both local and remote ODUs

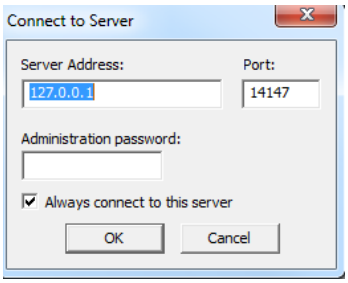
- Verify management access from remote NMS station

Appendix A: FileZilla Server Installation and Setup

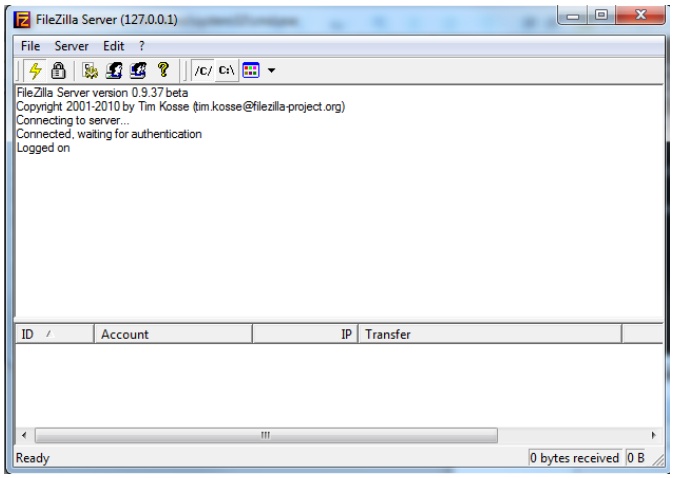
1. Download FileZilla Server from https://filezilla-project.org/download.php?type=server.

After downloading the file, run setup and use default configuration (select “Next”, “Accept” and “Install” when prompted). Select “Finish” when installation is completed.

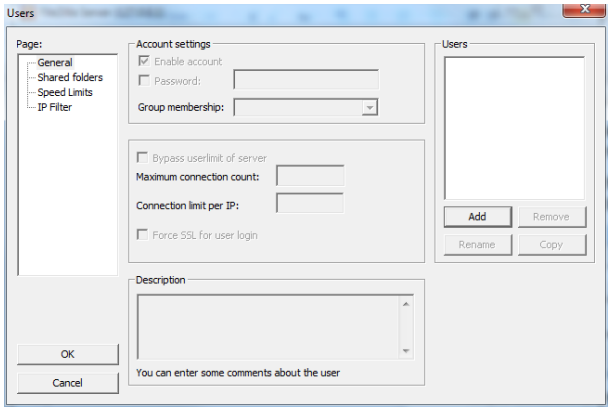
2. Launch the “FileZilla Server Interface” application. The “Connect to Server” screen is displayed. Leave the default settings and click “OK”.



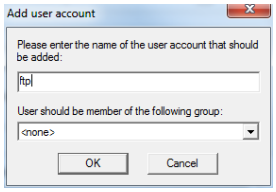
3. Launch the “FileZilla Server” interface screen will be displayed.



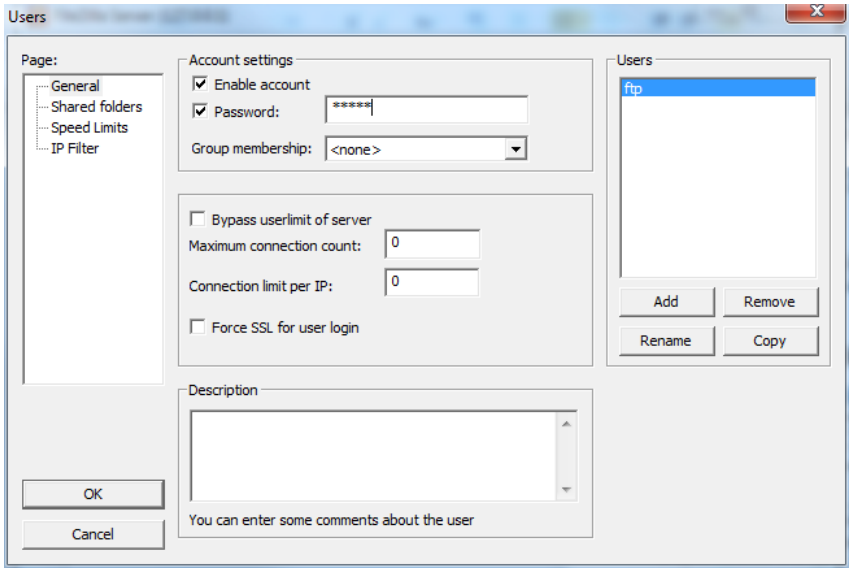
4. Select “Edit” and then “Users”. The “User” screen will be displayed.



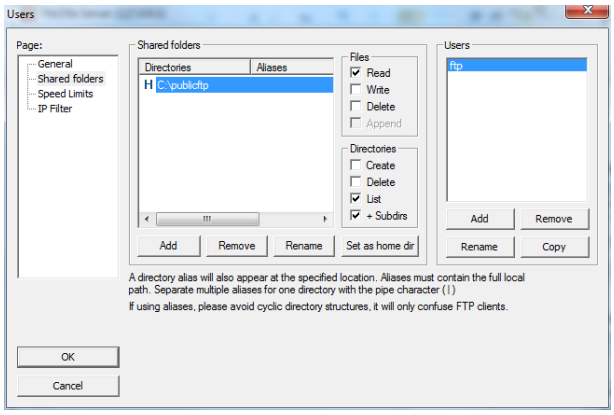
5. Under “Page: General” click Add and enter user ftp and click OK.



6. Under “Account Settings” check the “Password” check-box and enter password admin.



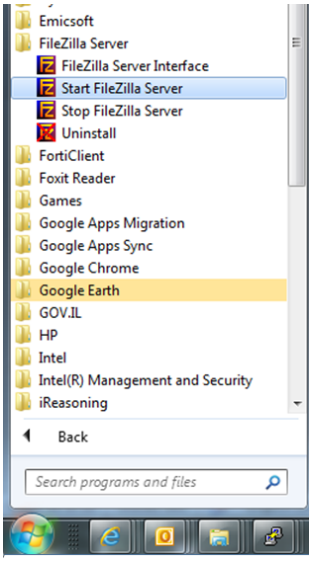
5.Under “Page: Shared Folder” click Add and select the ftp root (Home) directory where the files will be stored.



7. Click OK to complete setup.

Running the File Zilla Server

1. Store the files under C:/publicftp (in the home path directory of the FTP server).
2. Start the FileZilla service from the start menu (Start → All Programs → FileZilla Server → Start FileZilla Server).



Appendix B: Open TFTP Server Installation and Setup

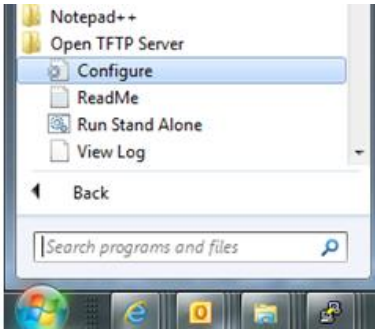
File transfer using FTP requires that the FTP service is not occupied by other application or services. In addition, some Firewall or Antivirus settings will block the FTP service.

In such cases, TFTP may be used as it is often more available and not blocked.

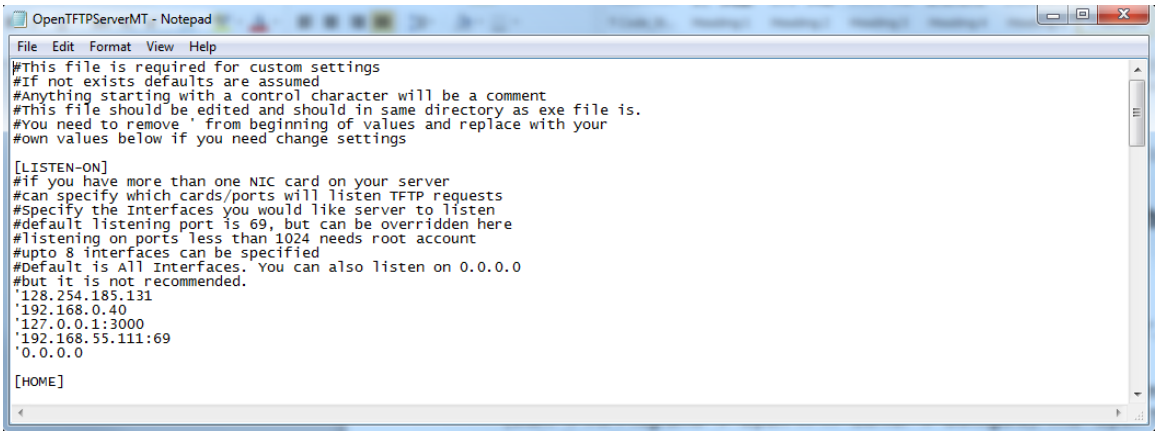
Note:

TFTP is supported on SW 5.0.0 or higher

1. Download Open TFTP Server from http://sourceforge.net/projects/tftpserver/?source=recommended .
   After downloading the file, run setup and use default configuration (select “Next”, “Accept” and “Install” when prompted). Select “Finish” when installation is completed.
2. Configure the Open TFTP Server by opening the configuration text file from the start menu (Start → All Programs → Open TFTP Server → Configure).



3. The “Open TFTP ServerMT config file will be opened.



4. Add the TFTP server IP address under the [LISTEN-ON] section and the root (home) directory where the file will be stored under the [HOME] section:

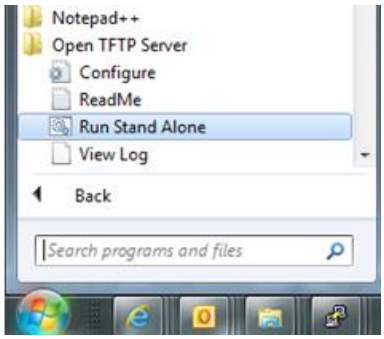
```
#This file is required for custom settings
#If not exists defaults are assumed
#Anything starting with a control character will be a comment
#This file should be edited and should in same directory as exe file is.
#You need to remove ' from beginning of values and replace with your
#own values below if you need change settings

[LISTEN-ON]
#if you have more than one NIC card on your server
#can specify which cards/ports will listen TFTP requests
#Specify the Interfaces you would like server to listen
#default listening port is 69, but can be overridden here
#listening on ports less than 1024 needs root account
#upto 8 interfaces can be specified
#Default is All Interfaces. You can also listen on 0.0.0.0
#but it is not recommended.
'128.254.185.131
'192.168.0.40
'127.0.0.1:3000
'192.168.55.111:69
'0.0.0.0
192.168.0.222     ←Add this line to indicate the server IP address
[HOME]
#You should specify home directory(s) here
#You can specify one directory as home
#directory, from where files will be served or
#deposited like:-
'c:\users\me\firmware\
#Alternatively if you want to specify multiple
#home directories, you need to use aliases
#like:-
'routers=d:\hda1\RouterImages\Images
'boot=e:\mnt\pc1\PXEBoot\Images
'installs=c:\hda5\installs
c:\publicftp\     ←Add this line to indicate where file is stored
```

Note that in this example we do not configure user or password.

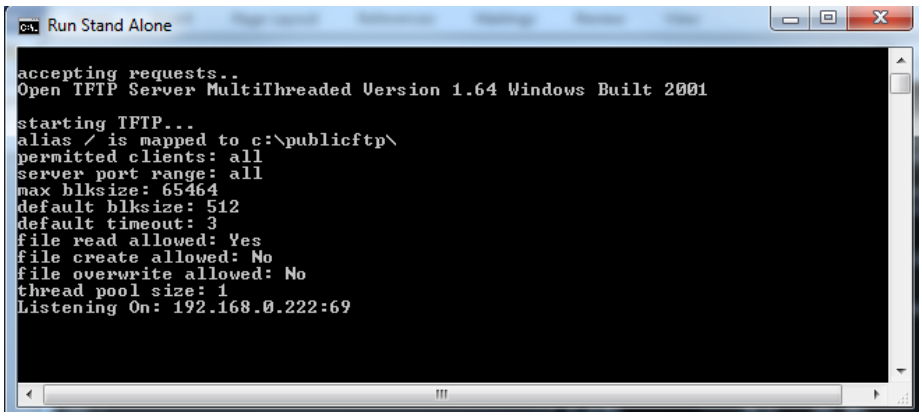
5. Close the txt file and save (**Exit → Save**).

Running the Open TFTP Server

1. Store the files under C:/publicftp (in the home path directory of the FTP server).
2. Start the Open TFTP service in stand-alone mode from the start menu (Start → All Programs → Open TFTP Server → Run Stand Alone).



3. The following batch screen will be displayed, indicating TFTP listening:



SW Download using TFTP

Use the CLI to load the license file:

```
ETH-1200> copy sw tftp://192.168.0.200/sw-uimage-3.0.0.6343

Done
.....
finished
```

Continue with SW upgrade steps as detailed in Sec 5.2 SW Upgrade – Using CLI.