



Quick Note 14

Secure File Upload Using PSCP

UK Support

November 2015

Contents

1	Introduction	3
1.1	Outline.....	3
1.2	Assumptions.....	3
1.3	Version.....	3
2	Configuration	4
2.1	Ethernet 0 LAN Configuration	4
2.2	Generate a Private Key for use with SSH.	5
2.3	Configure the SSH Server	6
3	Example Scenario	7
3.1	Copy the firmware files to your PC.....	7
3.2	Check the Current Version of Firmware	7
3.3	Upload Files using PSCP and Upgrade the Firmware.	8
3.4	File Upload	9
3.5	Update the Boot loader	10
3.6	Upload the Web File.....	10
3.7	SCAN	10
3.8	Check the New Version of Firmware	11
4	TransPort router Configuration Files	12

1 INTRODUCTION

1.1 Outline

This document shows how to upload firmware files over a secure connection using **PSCP** and upgrading of the firmware. **PSCP** is a command-line secure file copy facility using **PuTTY**.

You can download the latest version of **PSCP** from the following link;

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

- The TransPort router's configuration is set to factory defaults
- The TransPort router's firmware version is 4.706 or later.
- The user has some prior experience of configuring a TransPort router
- The user has prior experience of upgrading TransPort firmware.
- The default username = **username** and password = **password**.
- The user has prior knowledge of **PSCP** and **PuTTY**.

This application note applies to;

Models shown: Digi Transport DR6410.

Other Compatible Models: All Digi Transport products.

Firmware versions: 4.706 and above.

Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

1.3 Version

Version Number	Status
1.0	Published
1.1	Rebranded & updated

2 CONFIGURATION

2.1 Ethernet 0 LAN Configuration

First configure an IP address on the router. This can be on any interface but in this example we use Ethernet port 0 of the TransPort router.

Configuration - Interfaces > Ethernet > ETH 0 > Configure

Configuration - Interfaces > Ethernet > ETH 0 > Configure

Configure: Ethernet 0

Description:

IP analysis:

Ethernet analysis:

DHCP client:

IP address:

Multihome additional consecutive addresses:

Mask:

Max Rx rate (kbps):

Max Tx rate (kbps):

Group:

DNS server:

Secondary DNS server:

Gateway:

Parameter	Setting	Description
IP Address:	10.1.19.1	Configures the IP address for the LAN
Mask:	255.255.0.0	Configures the subnet mask for the LAN

2.2 Generate a Private Key for use with SSH.

Configuration - Security > Certificates > Utilities

Select a key size and file name for the private key file.

NB: The private key file can be given any name providing it ends with '.pem' and does not exceed 8 characters before the dot. For private key files it is recommended you follow the **priv*.pem** convention as a file prefixed with '**priv**' has increased security as it can not be copied or viewed.

Configuration - Security > Certificates > Utilities

Certificate utilities

New Key Size: 1024

Private key filename: privssh.pem

Save in SSHv1 format:

Certificate request filename: View

Generate Private Key Generate Certificate Request

Parameter	Setting	Description
New Key Size:	1024	Configures the size of the private key in KB
Private Key Filename:	privssh.pem	Configures the name of the private key file
Generate Private Key	Button	Generates the private key on the router's flash

After a few seconds, the results screen should be shown, confirming the key was generated.

Configuration - Security > Certificates > Utilities

Idle

Results:

```
Starting 1024 bit key generation. Please wait. This may take some time...
```

```
Key generated, saving to FLASH file privssh.pem
```

```
Closing file
```

```
Private key file created
```

```
All tasks completed
```

2.3 Configure the SSH Server

Configuration - Management > SSH Server > SSH Server 0

Configuration - Management > SSH Server > SSH Server 0

Configure: SSH Server 0

Server port:

Number of listening sockets:

Version 1.5 enabled:

Version 2.0 enabled:

Host key #1 filename:

Host key #2 filename:

Maximum login time (secs):

Maximum login attempts:

Compression level:

Port forwarding enabled:

Command session host:

Command session port:

V1 options

Server key bits:

V2 options

Actively start key exchange:

Rekey Kbytes:

Encryption 3-DES preference (0=disabled):

Encryption AES 128 bit preference (0=disabled):

Encryption AES 192 bit preference (0=disabled):

Encryption AES 256 bit preference (0=disabled):

MAC MD5 preference (0=disabled):

MAC MD5-96 preference (0=disabled):

MAC SHA1 preference (0=disabled):

MAC SHA1-96 preference (0=disabled):

Debug output:

Parameter	Setting	Description
Host key # 1 filename:	privssh.pem	Enter the name of the private key file
Rekey Kbytes:	1024	specify the amount of data that is allowed to pass over the encrypted link before a new set of keys must be negotiated (SSH V2 only)

The router configuration is now complete, you can now use PSCP to copy files to the router.

3 EXAMPLE SCENARIO

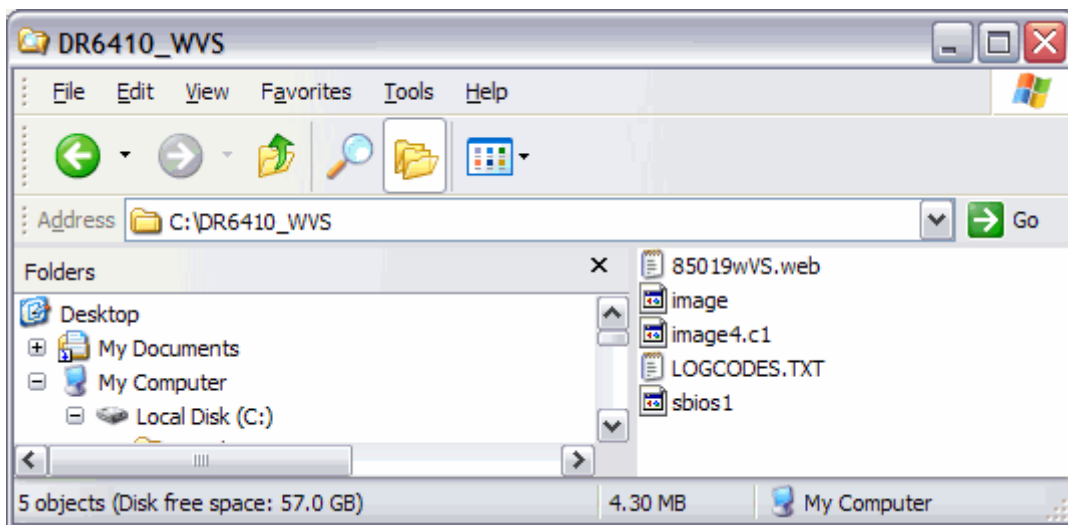
The following pages show how PSCP could be used to upgrade the routers firmware.

3.1 Copy the firmware files to your PC

From the Digi website, download the appropriate firmware files to your PC and remember where you saved them. It's better to keep the file path as short as possible as this needs to be entered manually into the command line during the upload.

In this example the files are save C:\DR6410_WVS directory

The file names are **85019wVS.web**, **image**, **image4.c1**, **logcodes.txt** and **sbios1**.



3.2 Check the Current Version of Firmware

Administration - Version info

Check the Software Build Version. Here the firmware version is 5011.

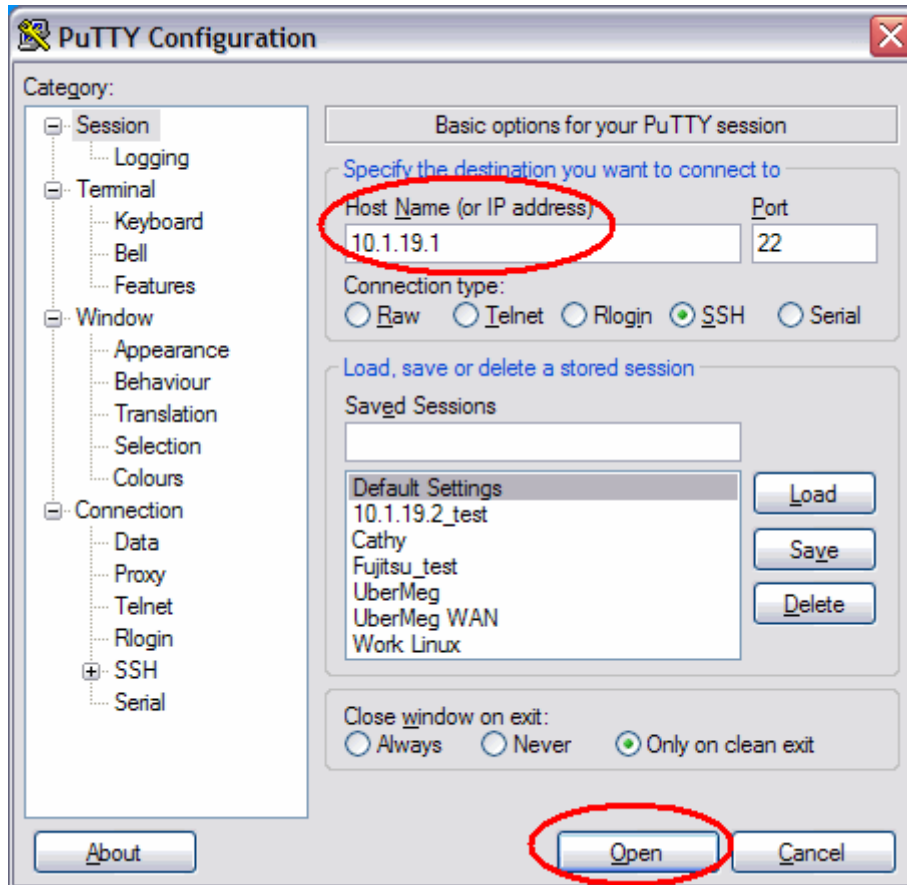
Sarian Systems. Sarian DR6410-HIA DSL2/2+ Router Ser#:74895
Software Build Ver5011, Mar 19 2008 04:14:40 8W

WEB Build	dr64x0
BIOS	ARM Sarian Bios Ver 4.83 v31 197MHz B128-M128-F300-O100000,0 MAC:00042d01248f
Async Driver	Revision: 1.19
Ethernet Port Isolate Driver	Revision: 1.11
ISDN ST 21150 Driver	Revision: 1.7
Firewall	Revision: 1.0
EventEdit	Revision: 1.0
Timer Module	Revision: 1.1
AAL	Revision: 1.0
ADSL	Revision: 1.0
(B)USBHOST	Revision: 1.0

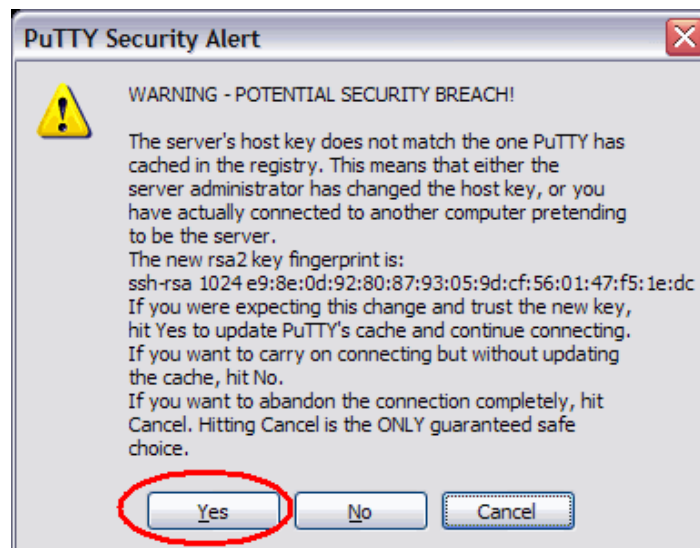
3.3 Upload Files using PSCP and Upgrade the Firmware.

To ensure there is enough room on the flash for additional files delete the file ending in '.web' via the command line.

Using PuTTY, enter the IP address of the TransPort router and click **Open**.



The first time you use PuTTY or a new private key you will see the following alert.



Click **Yes** to accept the router's host key.

At the command prompt Login to the router with a username password which has 'super user' privileges. We will use the default username = **username** and password = **password**.

Once logged in run the command line **del <filename>.web**

Hint: To show the name of the web file type **dir<enter>** to see a list of all files names.

A screenshot of a PuTTY terminal window titled "10.1.19.1 - PuTTY". The terminal shows a login sequence: "login as: username" followed by "username@10.1.19.1's password:". Below that, the user "ss74895" enters the command "del 85011wvs.web", and the terminal responds with "OK". A green cursor is visible on the line following "OK".

```
10.1.19.1 - PuTTY
login as: username
username@10.1.19.1's password:

ss74895>del 85011wvs.web
OK
█
```

NB: Once this file is deleted you will not be able to view the router's web interface.

3.4 File Upload

Download the latest 'pscp.exe' and copy it to the directory on your PC at the location where your DOS prompt usually opens.

To upload the files the PSCP command line usage in this example will be;

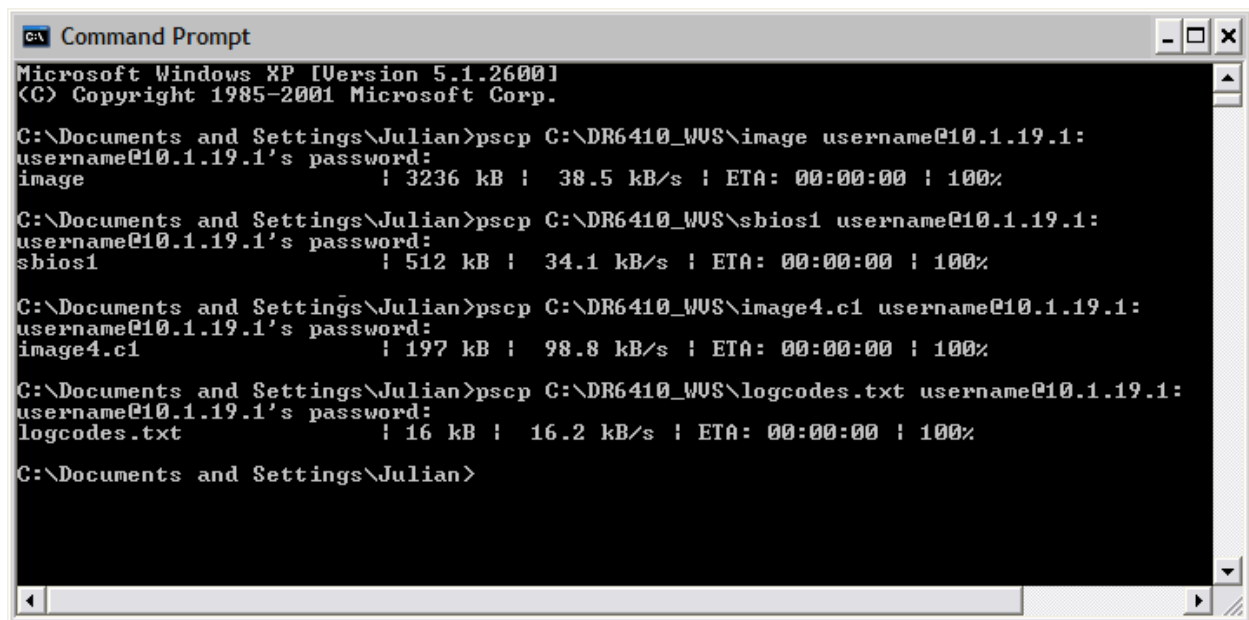
pscp <source path>\<source file> [user@]host:

For a full list of PSCP commands go here:

<http://the.earth.li/~sgtatham/putty/0.60/html/doc/Chapter5.html>

Upload all firmware files except the .web file using the following commands. You will be asked for the password (= password) for each file.

```
pscp C:\DR6410_wvs\image username@10.1.19.1:
pscp C:\DR6410_wvs\sbios1 username@10.1.19.1:
pscp C:\DR6410_wvs\image4.c1 username@10.1.19.1:
pscp C:\DR6410_wvs\logcodes.txt username@10.1.19.1:
```



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Julian>pscp C:\DR6410_WUS\image username@10.1.19.1:
username@10.1.19.1's password:
image                | 3236 kB | 38.5 kB/s | ETA: 00:00:00 | 100%

C:\Documents and Settings\Julian>pscp C:\DR6410_WUS\sbios1 username@10.1.19.1:
username@10.1.19.1's password:
sbios1               | 512 kB | 34.1 kB/s | ETA: 00:00:00 | 100%

C:\Documents and Settings\Julian>pscp C:\DR6410_WUS\image4.c1 username@10.1.19.1:
username@10.1.19.1's password:
image4.c1            | 197 kB | 98.8 kB/s | ETA: 00:00:00 | 100%

C:\Documents and Settings\Julian>pscp C:\DR6410_WUS\logcodes.txt username@10.1.19.1:
username@10.1.19.1's password:
logcodes.txt         | 16 kB | 16.2 kB/s | ETA: 00:00:00 | 100%

C:\Documents and Settings\Julian>
```

3.5 Update the Boot loader

Close the PSCP DOS prompt and connect to the command line using PuTTY.

Run the command `move sbios1 sbios`



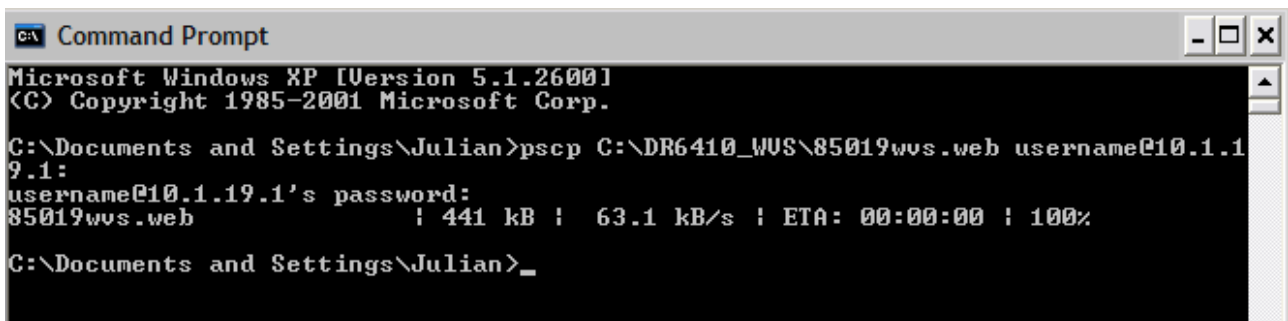
```
10.1.19.1 - PuTTY
login as: username
username@10.1.19.1's password:

ss74895>move sbios1 sbios
OK
```

3.6 Upload the Web File

Close the PuTTY session and upload the *.web file using PSCP.

`pscp C:\DR6410_wvs\85019wvs.web username@10.1.19.1:`



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Julian>pscp C:\DR6410_WUS\85019wvs.web username@10.1.19.1:
username@10.1.19.1's password:
85019wvs.web         | 441 kB | 63.1 kB/s | ETA: 00:00:00 | 100%

C:\Documents and Settings\Julian>
```

3.7 SCAN

Now that all firmware files are uploaded and the boot loader is updated, check the integrity of the files by issuing the `scan` command via the command line using PuTTY.

```

10.1.19.1 - PuTTY
login as: username
username@10.1.19.1's password:

ss74895>scan
Please wait...
  direct ....ok
  sbios ....ok
  mirror ....ok
LOGCODES.TXT ....ok
  sregs.dat ....ok
85019wvs.web ....ok
  templog.c1 ....ok
  image ....ok, data ok
  image4.c1 ....ok, data ok
  config.fac ....ok
  x3prof ....ok
  fw.txt ....ok
  config.jm ....ok

```

If there are no BAD CRC's then run the reboot command to powercycle the router and apply the new firmware.

3.8 Check the New Version of Firmware

Administration - Version info

Check the Software Build Version. The firmware version is now showing 5019.

Sarian Systems. Sarian DR6410-HIA DSL2/2+ Router
 Ser#:74895
 Software Build Ver5019. May 7 2008 13:06:10 8W

WEB Build	dr64x0
BIOS	ARM Sarian Bios Ver 4.90 v31 197MHz B128-M128-F300-O100000,0 MAC:00042d01248f
Async Driver	Revision: 1.19
Ethernet Port Isolate Driver	Revision: 1.11
ISDN ST 21150 Driver	Revision: 1.7
Firewall	Revision: 1.0
EventEdit	Revision: 1.0
Timer Module	Revision: 1.1
AAL	Revision: 1.0
ADSL	Revision: 1.0
(B)USBHOST	Revision: 1.0

4 TRANSPORT ROUTER CONFIGURATION FILES

The configuration file used for this quick note.

```
eth 0 IPAddr "10.1.19.1"
eth 0 mask "255.255.0.0"
adsl 0 watchdog OFF
lapb 0 ans OFF
lapb 2 dtemode 2
lapb 3 dtemode 2
def_route 0 ll_ent "PPP"
def_route 0 ll_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 4
ppp 0 use_modem 3
ppp 1 IPAddr "0.0.0.0"
ppp 1 username "Enter ADSL Username"
ppp 1 epassword "Dm1DbV9VH3s="
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 lliface "AAL"
ppp 4 l_acfc ON
ppp 4 l_pfc ON
ppp 4 IPAddr "1.2.3.5"
ppp 4 IPmin "10.10.10.0"
ppp 4 username "Enter PSTN Username"
ppp 4 timeout 60
ppp 4 use_modem 3
ana 0 anon ON
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 200
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "SS.6000r"
cmd 0 asyled_mode 1
cmd 0 tremto 1200
user 0 name "username"
user 0 epassword "KD5lSVJDVVg="
user 0 access 0
user 1 name "Sarian"
user 1 epassword "HA0gDhQc"
user 1 access 0
user 2 epassword "Kzp1SEBY"
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
local 0 transaccess 2
ssh 0 hostkey1 "privssh.pem"
ssh 0 rekeykbytes 1024
```