



Quick Note 14

Secure File Upload Using PSCP

UK Support
August 2011

Contents

1	Introduction.....	2
1.1	Outline.....	2
1.2	Assumptions	2
1.3	Version.....	3
2	Configuration.....	3
2.1	Ethernet 0 LAN configuration.....	3
2.2	Generate a private key for use with SSH.....	3
2.3	Configure the SSH Server.....	5
3	Example Scenario	6
3.1	Copy the firmware files to your PC.....	6
3.2	Check the current version of firmware	6
3.3	Configure PuTTY and delete the existing web file.....	7
3.4	Upload files with PSCP.....	8
3.5	Update the boot loader.....	9
3.6	Upload the web file	9
3.7	Check file integrity.....	9
3.8	Check the new version of firmware.....	10
4	TransPort Router Configuration Files.....	11

1 INTRODUCTION

1.1 Outline

This document shows how to upload files to a TransPort router over a secure connection using **PSCP** in order to upgrade its 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 5.123 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:

Model shown: Digi Transport DR64 MkII.

Other Compatible Models: All Digi Transport products.

Firmware versions: 5.123 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
1.2	Updated for new Web GUI

2 CONFIGURATION

2.1 Ethernet 0 LAN configuration

Configuration - Network > Interfaces > Ethernet > ETH 0

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

Configuration - Network > Interfaces > Ethernet > ETH 0

▼ Interfaces

▼ Ethernet

▼ ETH 0 - LAN 0

Description: LAN 0

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address: 10.1.41.1

Mask: 255.255.0.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

► Advanced

► QoS

► VRRP

Apply

Parameter	Setting	Description
IP Address	10.1.41.1	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

Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates

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

Note: 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 because it cannot be copied or viewed.

Administration - X.509 Certificate Management > IPsec/SSH/HTTPS Certificates

▶ Certificate Authorities (CAs)
▶ IPsec/SSH/HTTPS Certificates
▼ Key Generation

Key filename:
Key size: bits

☐ Save in SSHv1 format

Parameter	Setting	Description
Key size	1024	Configures the size of the private key in KB
Key filename	privSSH.pem	Configures the name of the private key file
Generate Key	Button	Generates the private key on the router's flash

After a few seconds the results screen should be shown, confirming that the key has been generated:

Key Generation 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 - Network > SSH Server > SSH Server 0

Configuration - Network > SSH Server > SSH Server 0

▼ SSH Server 0

☒ Enable SSH Server

Use TCP port: 22

Allow up to 5 connections

Host Key 1 Filename: privSSH.pem

Host Key 2 Filename:

Maximum login time: 60 seconds

Maximum login attempts: 3

Use Deflate compression: ☐ No
☒ Yes, level 6

☒ Enable Port Forwarding

Command Session IP Address: Port: 0

☐ Enable support for SSH v1.5

☒ Enable support for SSH v2.0

☒ Actively start key exchange

Rekey: ☐ Never
☒ After 1024 KBytes of data have been transferred

Encryption Preferences:

3DES: 1

AES (128 bits): 1

AES (192 bits): 1

AES (256 bits): 1

Authentication Preferences:

MAC MD5: 1

MAC MD5-96: 1

MAC SHA1: 1

MAC SHA1-96: 1

☐ Enable Debug

Parameter	Setting	Description
Host Key 1 Filename	privssh.pem	Enter the name of the private key file generated in the previous step
Rekey After n 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.

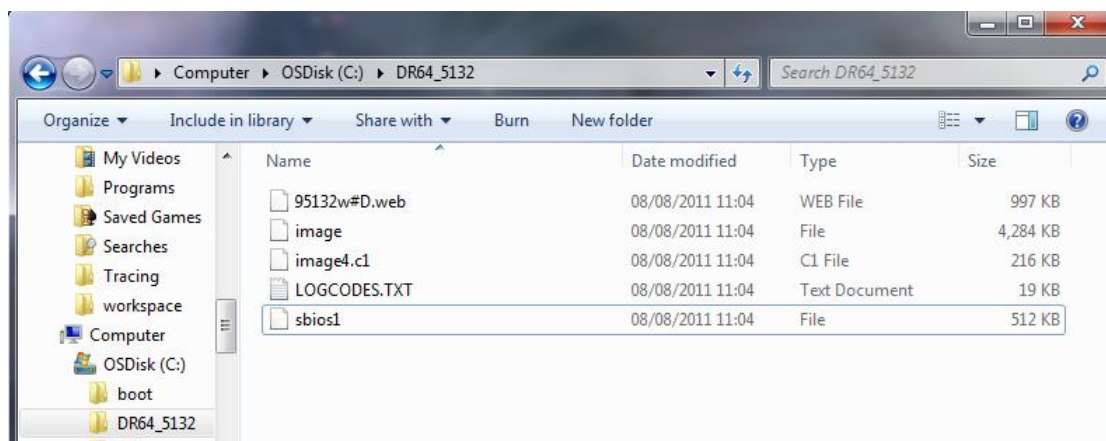
3 EXAMPLE SCENARIO

The following pages show how PSCP could be used to upgrade the router's 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 saved in the directory **C:\DR64_5132** and the file names are **95132w#D.web**, **image**, **image4.c1**, **LOGCODES.TXT** and **sbios1**:



3.2 Check the current version of firmware

Administration - System Information

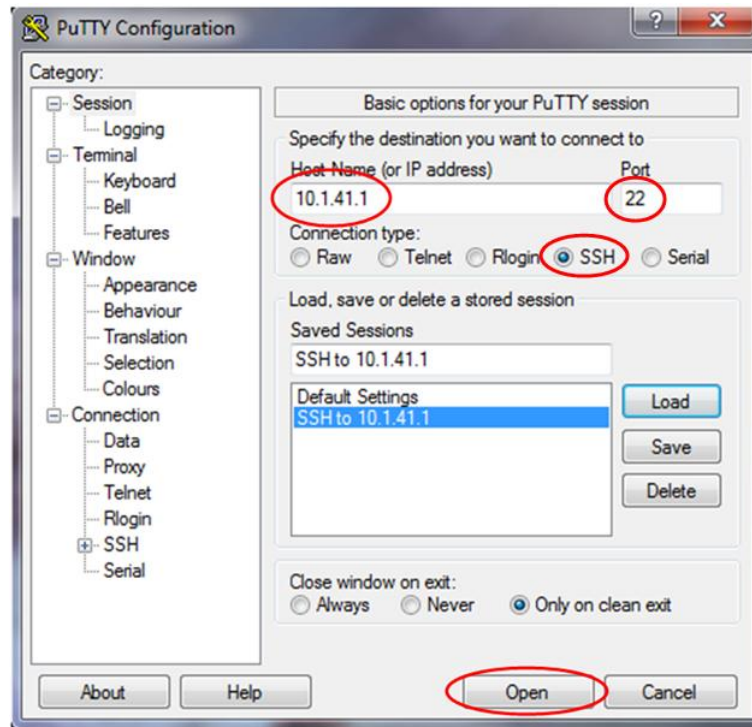
Here the firmware version is 5130:

Administration - System Information	
Model:	TransPort DR64
Part Number:	DR64-EXA1-DE2-XX
Ethernet 0 MAC Address:	00:04:2D:02:BE:B3
Firmware Version:	5130 \$ (Jun 3 2011 10:46:32)
SBIOS Version:	6.06
Build Version:	9W
HW Version:	7503a

3.3 Configure PuTTY and delete the existing web file

To ensure that there is enough room in the router's flash memory for additional files, delete the file ending in **web** via the command line.

Using PuTTY, enter the IP address of the TransPort router, ensure that the connection type is set to SSH (port 22) and click **Open**:



If the device that you are connecting to has a new private key, you will see the following alert:

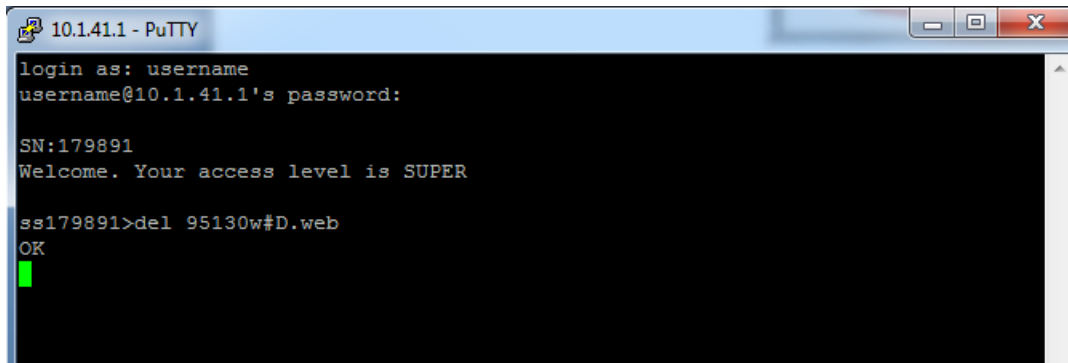


Click **Yes** to accept the router's host key.

At the command prompt login to the router with a username and password which has 'super user' privileges. In this example we use the defaults: username = **username** and password = **password**. Once logged in, run the CLI command **del <filename>.web**

Hint: To find the name of the web file, type **dir<enter>** to see a list of all files on the router.

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



```
10.141.1 - PuTTY
login as: username
username@10.1.41.1's password:

SN:179891
Welcome. Your access level is SUPER

ss179891>del 95130w#D.web
OK
```

3.4 Upload files with PSCP

Download the latest version of '**pscp.exe**' and copy it to the location on your PC where your Windows command prompt usually opens. Alternatively, use the '**cd**' command to change directory to where '**pscp.exe**' is located.

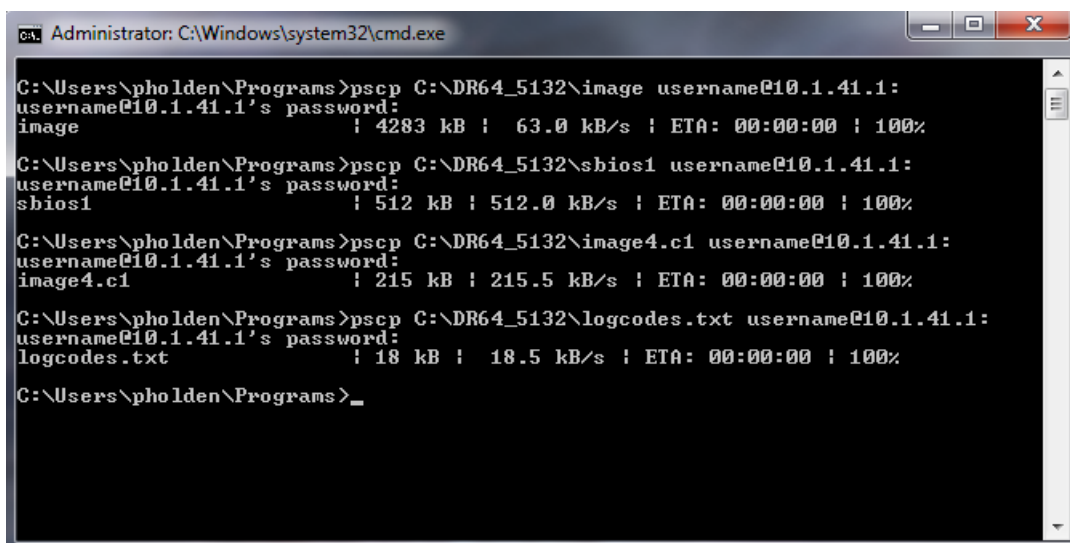
To upload the files the PSCP command line usage in this example will be:

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

For a full list of PSCP commands please see: <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:\DR64_5132\image username@10.1.41.1:
pscp C:\DR64_5132\sbios1 username@10.1.41.1:
pscp C:\DR64_5132\image4.c1 username@10.1.41.1:
pscp C:\DR64_5132\logcodes.txt username@10.1.41.1:
```



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\pholden\Programs>pscp C:\DR64_5132\image username@10.1.41.1:
username@10.1.41.1's password:
image                               | 4283 kB | 63.0 kB/s | ETA: 00:00:00 | 100%

C:\Users\pholden\Programs>pscp C:\DR64_5132\sbios1 username@10.1.41.1:
username@10.1.41.1's password:
sbios1                              | 512 kB | 512.0 kB/s | ETA: 00:00:00 | 100%

C:\Users\pholden\Programs>pscp C:\DR64_5132\image4.c1 username@10.1.41.1:
username@10.1.41.1's password:
image4.c1                           | 215 kB | 215.5 kB/s | ETA: 00:00:00 | 100%

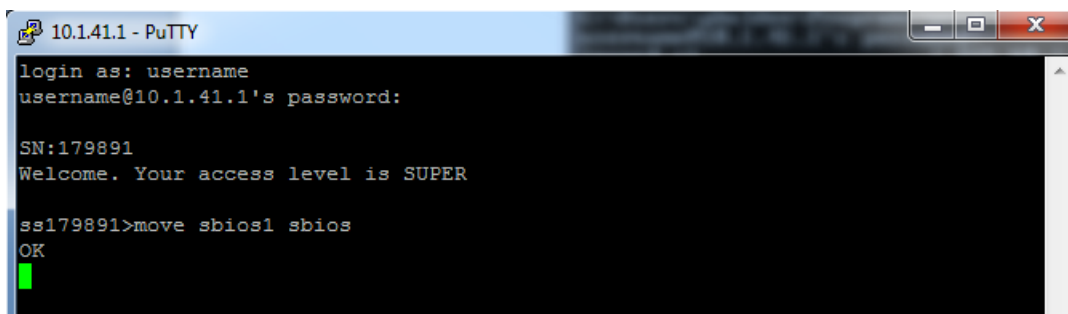
C:\Users\pholden\Programs>pscp C:\DR64_5132\logcodes.txt username@10.1.41.1:
username@10.1.41.1's password:
logcodes.txt                        | 18 kB | 18.5 kB/s | ETA: 00:00:00 | 100%

C:\Users\pholden\Programs>_
```


3.5 Update the boot loader

Close the PSCP command prompt and connect to the router's command line using PuTTY.

Run the command: **move sbios1 sbios**



```
10.1.41.1 - PuTTY
login as: username
username@10.1.41.1's password:

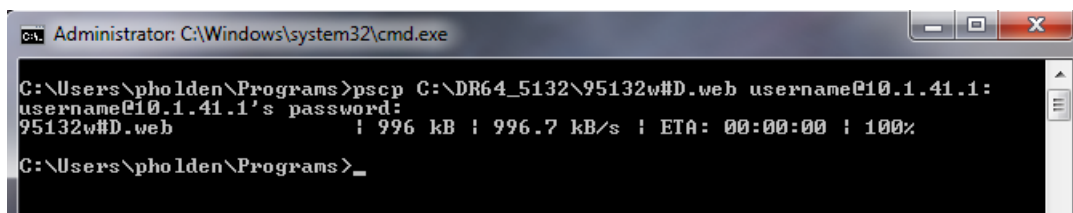
SN:179891
Welcome. Your access level is SUPER

ss179891>move sbios1 sbios
OK
```

3.6 Upload the web file

Close the PuTTY session, then upload the web file using the following PSCP command:

pscp C:\DR64_5132\95132w#D.web username@10.1.41.1:



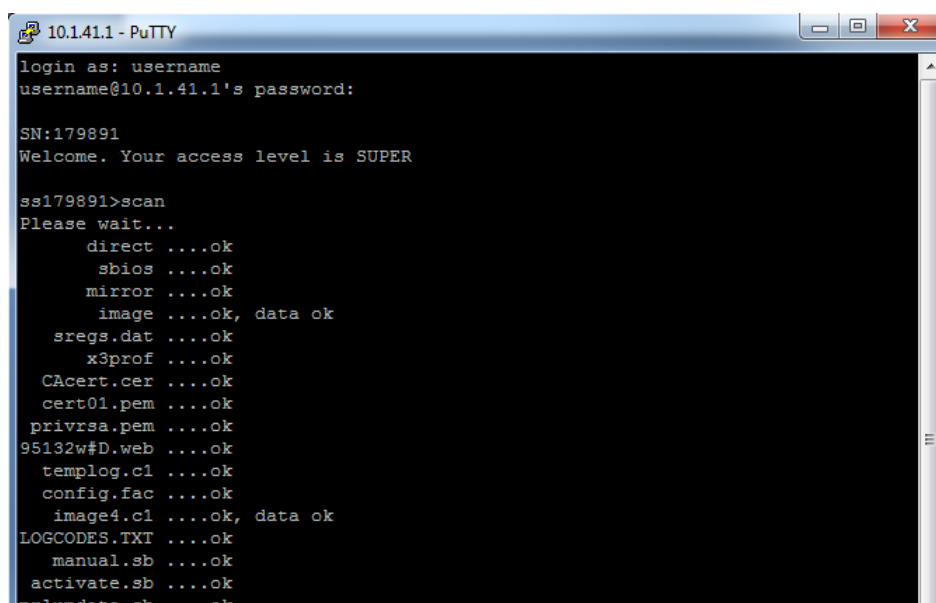
```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\pholden\Programs>pscp C:\DR64_5132\95132w#D.web username@10.1.41.1:
username@10.1.41.1's password:
95132w#D.web          ! 996 kB ! 996.7 kB/s ! ETA: 00:00:00 ! 100%

C:\Users\pholden\Programs>_
```

3.7 Check file integrity

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 router's command line using **PuTTY**:



```
10.1.41.1 - PuTTY
login as: username
username@10.1.41.1's password:

SN:179891
Welcome. Your access level is SUPER

ss179891>scan
Please wait...
  direct ....ok
  sbios ....ok
  mirror ....ok
  image ....ok, data ok
  sregs.dat ....ok
  x3prof ....ok
  CAcert.cer ....ok
  cert01.pem ....ok
  privrsa.pem ....ok
  95132w#D.web ....ok
  templog.c1 ....ok
  config.fac ....ok
  image4.c1 ....ok, data ok
  LOGCODES.TXT ....ok
  manual.sb ....ok
  activate.sb ....ok
  prlupdate.sb ....ok
```

If there are no BAD CRCs then run the **reboot** command to power cycle the router, so that the new firmware is loaded.

3.8 Check the new version of firmware

Administration - System Information

The firmware version is now showing 5132:

Administration - System Information	
Model:	TransPort DR64
Part Number:	DR64-EXA1-DE2-XX
Ethernet 0 MAC Address:	00:04:2D:02:BE:B3
Firmware Version:	5132 \$ (Jul 15 2011 23:42:41)
SBIOS Version:	6.20
Build Version:	9W
HW Version:	7503a

4 TRANSPORT ROUTER CONFIGURATION FILES

The configuration file used for this quick note.

```
eth 0 descr "LAN 0"
eth 0 IPaddr "10.1.41.1"
eth 0 mask "255.255.0.0"
eth 0 gateway "10.1.2.100"
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
eth 4 do_nat 2
eth 5 descr "ATM PVC 1"
eth 5 do_nat 2
eth 6 descr "ATM PVC 2"
eth 6 do_nat 2
eth 7 descr "ATM PVC 3"
eth 7 do_nat 2
eth 8 descr "ATM PVC 4"
eth 8 do_nat 2
eth 9 descr "ATM PVC 5"
eth 9 do_nat 2
eth 10 descr "ATM PVC 6"
eth 10 do_nat 2
eth 11 descr "ATM PVC 7"
eth 11 do_nat 2
eth 12 descr "Logical"
eth 13 descr "Logical"
eth 14 descr "Logical"
eth 15 descr "Logical"
eth 16 descr "Logical"
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 3 asyport 7
lapb 3 mux_0710 ON
lapb 4 dtemode 0
lapb 4 dlc 1
lapb 4 asyport 7
lapb 4 virt_async "mux0"
lapb 4 mux_0710 ON
lapb 5 dtemode 0
lapb 5 dlc 2
lapb 5 asyport 7
lapb 5 virt_async "mux1"
lapb 5 mux_0710 ON
lapb 6 dtemode 0
lapb 6 dlc 3
lapb 6 asyport 7
lapb 6 virt_async "mux2"
lapb 6 mux_0710 ON
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
def_route 1 ll_ent "eth"
def_route 1 ll_add 4
def_route 2 ll_ent "PPP"
def_route 2 ll_add 3
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
ppp 0 timeout 300
ppp 1 name "ADSL"
ppp 1 lliface "AAL"
```

```

ppp 1 username "Enter ADSL Username"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 immoos ON
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 3 name "W-WAN (Edge 2.5G)"
ppp 3 phonenum "*98*1#"
ppp 3 username "ENTER WWAN Username"
ppp 3 epassword "KD5lSVJDVVg="
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 use_modem 1
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
modemcc 0 asy_add "mux1"
modemcc 0 info_asy_add "mux2"
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.Goes.Here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.Goes.Here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 2 asy_add "mux0"
modemcc 2 link_retries 10
ana 0 anon ON
ana 0 llon ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
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
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF

```