Preparative Procedures (AGD_PRE)

for LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN

Version 1.8

Release

LANCOM Systems GmbH

Adenauer Str. 20/B2
52146 Würselen
Germany

Document History

Date	Version	Editor	Change
07.02.2012	0.1	SKörber	Document creation
10.02.2012	1.0	SKörber	Release Version
21.03.2012	1.1	SKörber	Feedback by SRC
04.06.2012	1.2	SKörber	Feedback by SRC and LANCOM
09.07.2012	1.3	SKörber	Added section about security advisories
20.11.2012	1.4	SKörber	Feedback by SRC & BSI
08.02.2013	1.5	SKörber	Feedback by LANCOM and SRC
19.03.2013	1.6	SKörber / TJansen	Feedback by SRC
03.04.2013	1.7	SKörber	Feedback BSI
11.04.2013	1.8	SKörber	Feedback LANCOM

Table of Contents

1. Preparative Procedures (AGD_PRE)

This document describes all necessary preparative procedures.

1.1. Acceptance Procedures

At the end of the certification process, the TOE will be downloadable as a firmware file at the LANCOM Systems website (https://www.lancom-systems.de/cc). The certification report will contain a SHA-256 hash of the firmware file. The user has to build a SHA-256 hash of the downloaded file to compare it to the hash mentioned in the certification report. Use the sha256sum tool on a Linux command line to obtain the hash of the downloaded firmware. This way, the user must make sure that the file is genuine.

1.1.1. Security Advisories

To receive information about security relevant bugs the administrator of the TOE must subscribe to the newsletter on the LANCOM Systems website (https://www.lancom-systems.de/cc).

1.2. Installation and Startup Procedures

This section describes the secure preparation of the operational environment and the secure installation of the TOE.

1.2.1. Preparation of the Operational Environment

As mentioned in the Security Target, the TOE requires an appropriate hardware to operate on. This hardware (i.e. LANCOM Router), has to be placed in a secure environment (e.g. server room) with no physical access possible by any unauthorized person. Only the administrator of the TOE must have physical access. He also has to make sure that the connection to an untrusted network is only controlled by the TOE and that the used computer is trustworthy. The administrator must ensure that any unintended bypass is prohibited (e.g. by preventing physical access and organizational means).

1.2.2. Installation of the TOE

Please be advised that the TOE must only be installed on one of the following devices as mentioned in the security target (ASE - Security Target):

Series	Model	HW platform	WAN	LAN	Device Category
178x	1781-4G (CC)	A	4G	4-Port Switch	VPN Business Router
	1781A (CC)	A	ADSL	4-Port Switch	
	1781A-3G (CC)	A	ADSL, 3G	4-Port Switch	
	1781A-4G (CC)	A	ADSL, 4G	4-Port Switch	
	1781EF (CC)	A	Ethernet, SFP	4-Port Switch	
x100	7100+ VPN (CC)	B	Ethernet	Ethernet	Large VPN Concentrator
	9100+ VPN (CC)	C	Ethernet	Ethernet	

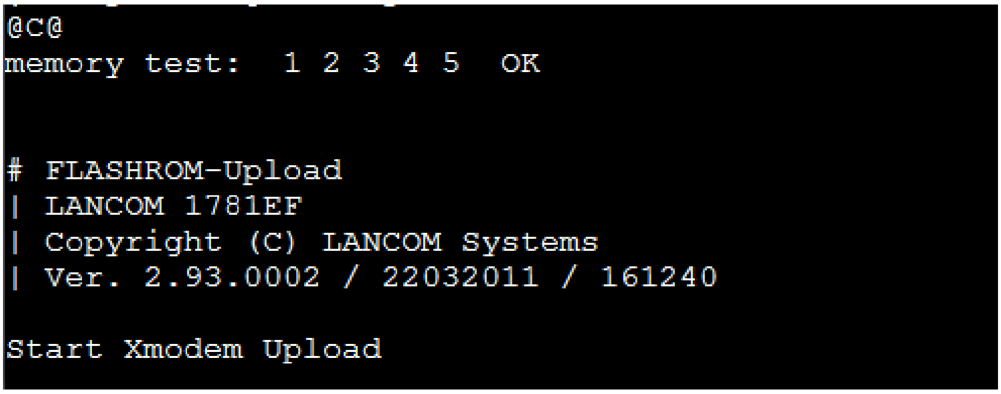
Before you start, please make sure you do not have any cable connected to the device and to run the device in a secure environment, which is not connected to any network during the installation of the TOE and during the initial configuration.

To install the TOE onto the hardware, the serial connector cable, the power plug and a terminal emulator (e.g.TerraTerm or any other management program of your choice) are required.

Please connect the serial connector cable to the config-port on the back of the device. Now start your favourite terminal emulator with the following parameters:

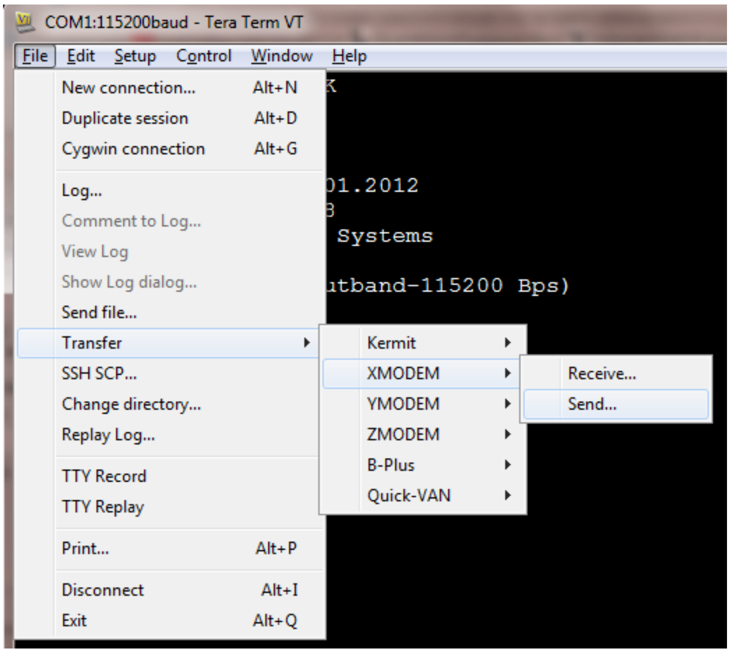
Interface:	COMx
Speed	115200
Data bits	8
Stop bits	1
Parity bits	none
Flow control	RTS/CTS

To upload the firmware and also perform a config reset at the same time, please make sure, that the router is not powered on. Now connect the power cable with the power supply and hold the reset button until you see the message “FLASHROM-Upload” in the terminal window.

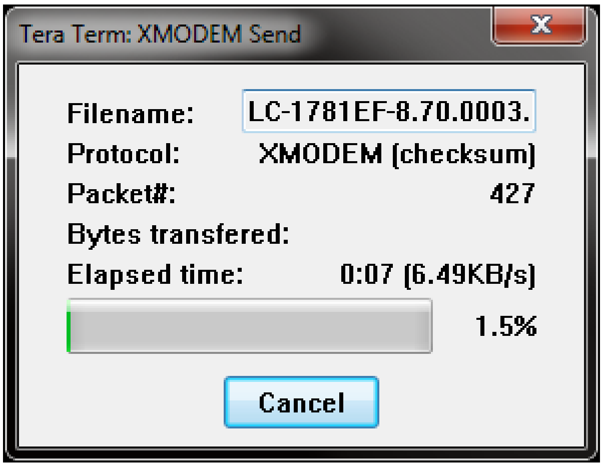


```
@C@
memory test:  1 2 3 4 5  OK


# FLASHROM-Upload
| LANCOM 1781EF
| Copyright (C) LANCOM Systems
| Ver. 2.93.0002 / 22032011 / 161240

Start Xmodem Upload
```

Now you are ready to upload the desired LCOS Release via XMODEM:



```
K


01.2012
3
 Systems

utband-115200 Bps)
```

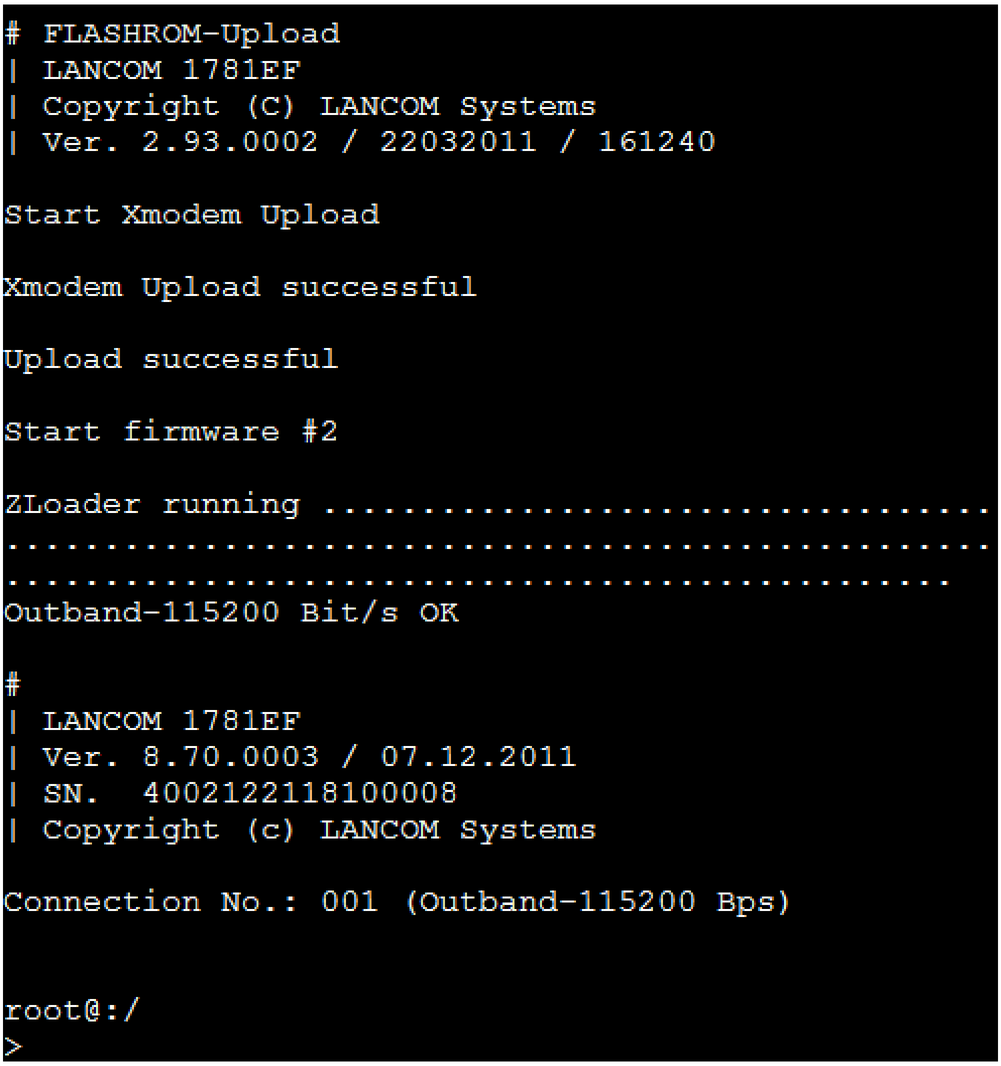


Tera Term: XMODEM Send

Filename: LC-1781EF-8.70.0003.
Protocol: XMODEM (checksum)
Packet#: 427
Bytes transfered:
Elapsed time: 0:07 (6.49KB/s)
1.5%

The firmware upload will also be signalized through the orange blinking Power LED of the LANCOM.

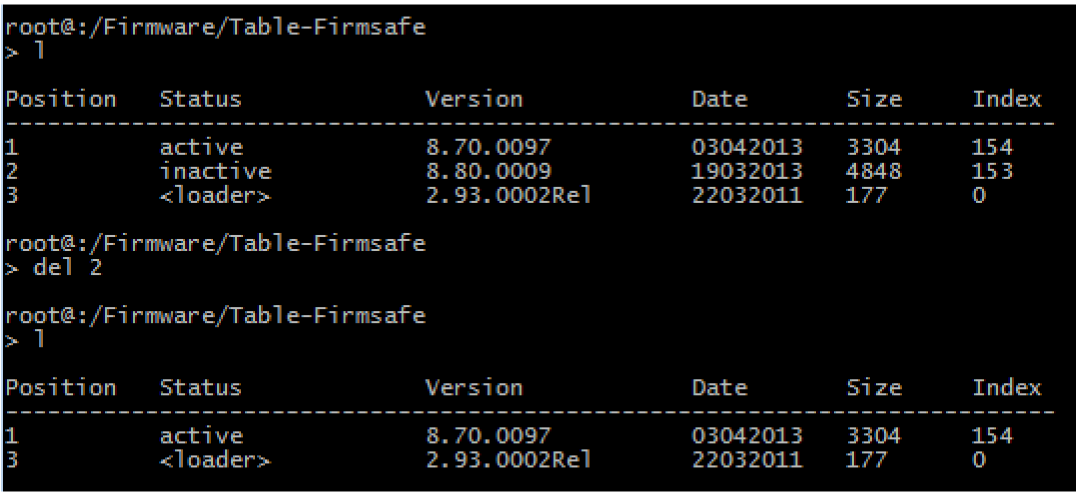
Once finished, the router will show that the firmware upload was successful and reboot with the new firmware. Verify that the version shown in the terminal matches the downloaded version.



```
# FLASHROM-Upload
| LANCOM 1781EF
| Copyright (C) LANCOM Systems
| Ver. 2.93.0002 / 22032011 / 161240

Start Xmodem Upload

Xmodem Upload successful

Upload successful

Start firmware #2

ZLoader running ..................................
..................................................
................................................
Outband-115200 Bit/s OK

#
| LANCOM 1781EF
| Ver. 8.70.0003 / 07.12.2011
| SN.  4002122118100008
| Copyright (c) LANCOM Systems

Connection No.: 001 (Outband-115200 Bps)


root@:/
>
```

You must also make sure that no other LCOS firmware is installed next to the LCOS 8.70CC. To delete any unwanted LCOS firmware head to /Firmware/Table-Firmsafe and run:

- “del 2”

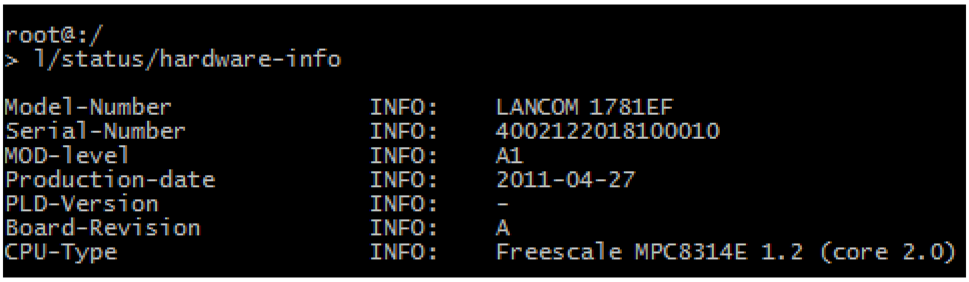


```
root@:/Firmware/Table-Firmsafe
> l

Position   Status              Version             Date        Size     Index
--------------------------------------------------------------------------------
1          active              8.70.0097           03042013    3304     154
2          inactive            8.80.0009           19032013    4848     153
3          <loader>            2.93.0002Rel        22032011    177      0

root@:/Firmware/Table-Firmsafe
> del 2

root@:/Firmware/Table-Firmsafe
> l

Position   Status              Version             Date        Size     Index
--------------------------------------------------------------------------------
1          active              8.70.0097           03042013    3304     154
3          <loader>            2.93.0002Rel        22032011    177      0
```

Note: You can only delete the inactive firmware!

Before starting with the initial configuration, please check that the CPU type matches your model name mentioned in the table above (1.2.2 – Installation of the TOE). You must do this by typing:

- “ls /status/hardware-info”



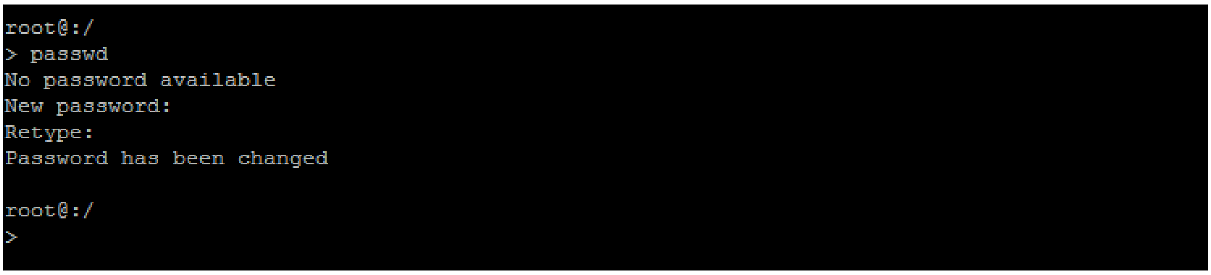
```
root@:/
> l/status/hardware-info

Model-Number              INFO:    LANCOM 1781EF
Serial-Number             INFO:    4002122018100010
MOD-level                 INFO:    A1
Production-date           INFO:    2011-04-27
PLD-Version               INFO:    -
Board-Revision            INFO:    A
CPU-Type                  INFO:    Freescale MPC8314E 1.2 (core 2.0)
```

1.2.3. Initial Configuration

Since we’re already connected via the serial connector cable, we now can start with the configuration of the LANCOM device.

The first thing to do is to set a password for root. This must be done by typing the command “passwd”. You must retype the new password to make sure, that there is no mistyping.

To ensure a proper protection of the user account root, a strong password (i.e. at least 8 characters containing alphabetic, numeric and special characters) must be used. The password must not be susceptible to dictionary attacks. The administrator of the TOE can change the password at any time. The new password must meet the same requirements.



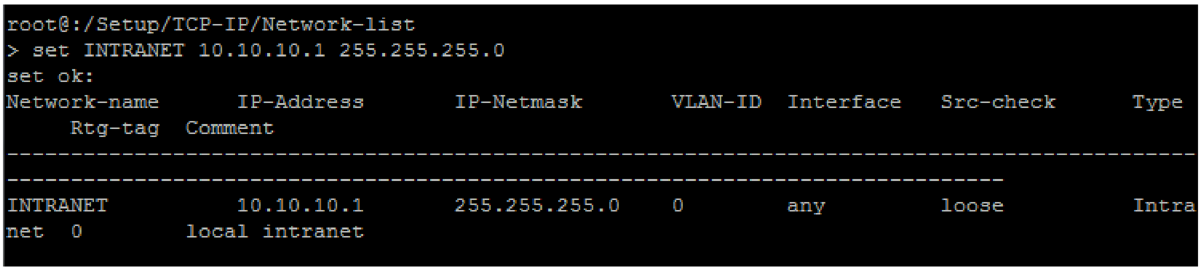
```
root@:/
> passwd
No password available
New password:
Retype:
Password has been changed

root@:/
>
```

Now you must start with the initial configuration. If at any point necessary you can reset your configuration by running “default –r” when you are in the top level directory “/”. This will reset the router configuration and set LCOS default values which are outside of the TOE. After that you must set the TOE specific settings which must be done by running “ccset”.

To manually set an IP Network, go to /Setup/TCP-IP/Network-List. There you must specify the IP-Address of your device and set the IP Network-Range.

A possible command might be:

- “set INTRANET 10.10.10.1 255.255.255.0”



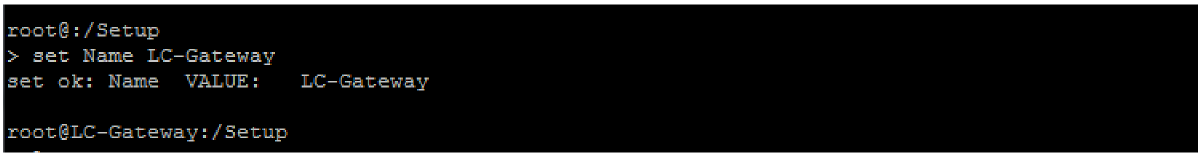
```
root@:/Setup/TCP-IP/Network-list
> set INTRANET 10.10.10.1 255.255.255.0
set ok:
Network-name      IP-Address       IP-Netmask       VLAN-ID  Interface   Src-check      Type
     Rtg-tag  Comment
----------------------------------------------------------------------------------------------
------------------------------------------------------------------------------
INTRANET          10.10.10.1       255.255.255.0    0        any         loose          Intra
net  0        local intranet
```

As mentioned in the Security Target, the use of VLAN-Tags is not used to provide additional security and therefore is not within the scope of the security evaluation. For further information regarding VLAN and its configuration check LCOS-MENU-860-EN.pdf (2.7.30.4 - VLAN-ID) and (P.2.32 – VLAN) as linked in AGD_OPE 1.4 (Further documentation).

If you want to give the device a name, you can set one in: /Setup.

A possible command might be:

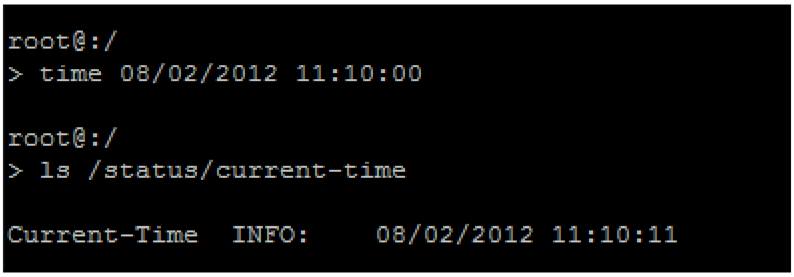
- “set Name LC-Gateway”



```
root@:/Setup
> set Name LC-Gateway
set ok: Name  VALUE:   LC-Gateway

root@LC-Gateway:/Setup
```

To make sure, that the device has a valid date and time, please use the following command:

- “time 08/02/2012 11:10:00” where the date format is MM/DD/YYYY hh:mm:ss



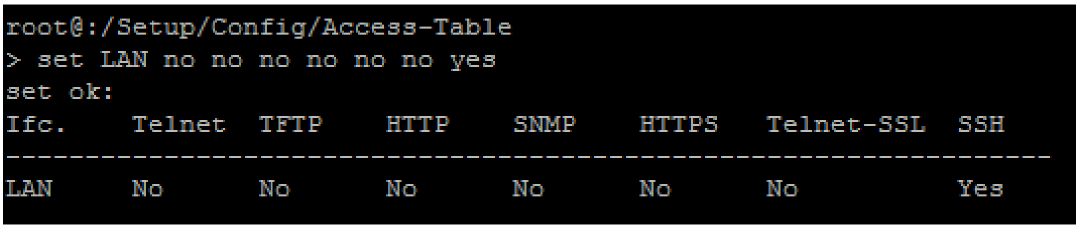
```
root@:/
> time 08/02/2012 11:10:00

root@:/
> ls /status/current-time

Current-Time  INFO:    08/02/2012 11:10:11
```

You must check the date and time with:

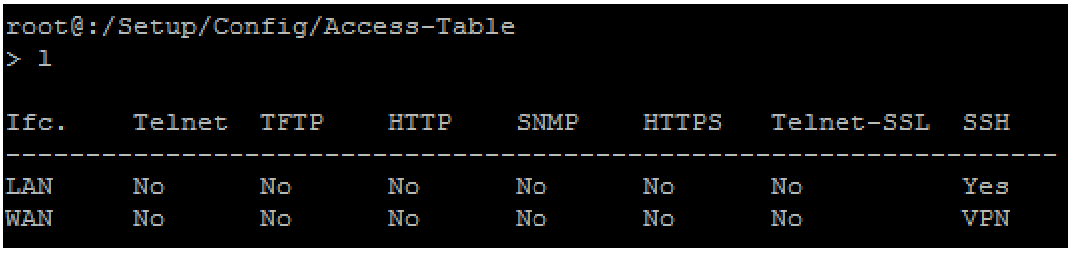
- “ls /status/current-time”

To allow a secure remote admin connection via command line, the use of SSHv2 from LAN can be enabled. Everything else must be set to “no”. If you also like to allow a SSHv2 connection from a trusted remote network, you can set the WAN access to “VPN”.

- “set /Setup/Config/Access-Table/LAN no no no no no no yes”
- set /Setup/Config/Access-Table/WAN no no no no no no no” or “set WAN no no no no no no VPN”



```
root@:/Setup/Config/Access-Table
> set LAN no no no no no no yes
set ok:
Ifc.    Telnet  TFTP    HTTP    SNMP    HTTPS   Telnet-SSL  SSH
-------------------------------------------------------------------
LAN     No      No      No      No      No      No          Yes
```

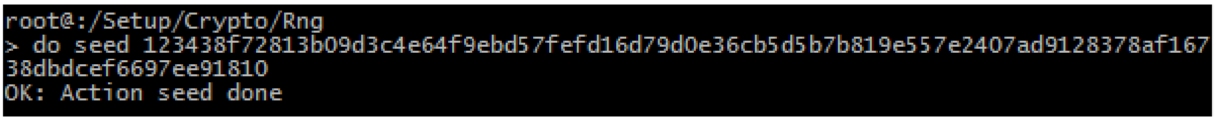


```
root@:/Setup/Config/Access-Table
> l

Ifc.    Telnet  TFTP    HTTP    SNMP    HTTPS   Telnet-SSL  SSH
-------------------------------------------------------------------
LAN     No      No      No      No      No      No          Yes
WAN     No      No      No      No      No      No          VPN
```

For the use of the software random number generator a unique random seed with high entropy[1] is required. To obtain the seed you need a certified product[2] like your passport, identity card or any other compatible hardware[3]. From your certified source of random numbers please obtain 96 characters in hexadecimal notation (48 bytes of random numbers).

Please go to "/Setup/Crypto/Rng". Once you have created these random numbers you must use them as a seed and enter them in a trusted environment. A trusted environment is either a serial connection, a SSHv2 session via a direct Ethernet link between the router and the trusted host or a SSHv2 session once the TOE is running in the evaluated configuration. Now use the serial connection to enter the seed as mentioned in the example below:

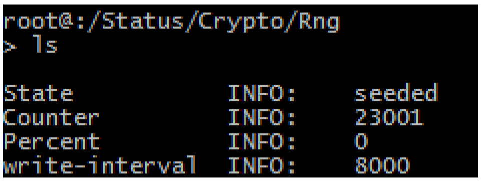
- "do seed 123438f72813b09d3c4e64f9ebd57fefd16d79d0e36cb5d5b7b819e557e2407ad9128378af167 38dbdcef6697ee91810"



```
root@:/Setup/Crypto/Rng
> do seed 123438f72813b09d3c4e64f9ebd57fefd16d79d0e36cb5d5b7b819e557e2407ad9128378af167
38dbdcef6697ee91810
OK: Action seed done
```

Please make sure that the state is now marked as "seeded" by entering "ls /status/crypto/rng" since it is the required state to operate to the TOE in the evaluated configuration. Other possible values for state are "pre-seeded", "seeded", "not-seeded", "needs-reseed" and "error". If the value of the state is "pre-seeded" or "not-seeded" you must enter a valid seed as mentioned above. If the value of the state is "needs-reseed" you must follow the instructions below. In case of an "error" state you must reboot the system and enter the seed again.

will be checked by cctest



```
root@:/Status/Crypto/Rng
> ls

State           INFO:    seeded
Counter         INFO:    23001
Percent         INFO:    0
write-interval  INFO:    8000
```

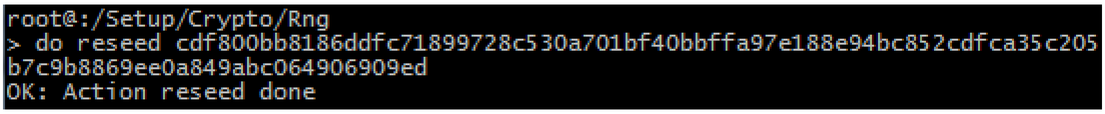
If the TOE reaches 99 percent ("ls /status/crypto/rng") or if you need to insert a new seed for the random number generator you must use the reseed function and obtain the new seed in the same way as the initial seed. The new seed must be entered in a trusted environment as mentioned above.

- "do reseed cdf800bb8186ddfc71899728c530a701bf40bbffa97e188e94bc852cdfca35c205b7c9b8869ee0 a849abc064906909ed"

[1] at least 100 bits

[2] containing at least a PTG.2 class physical random number generator (see AIS 20/31)

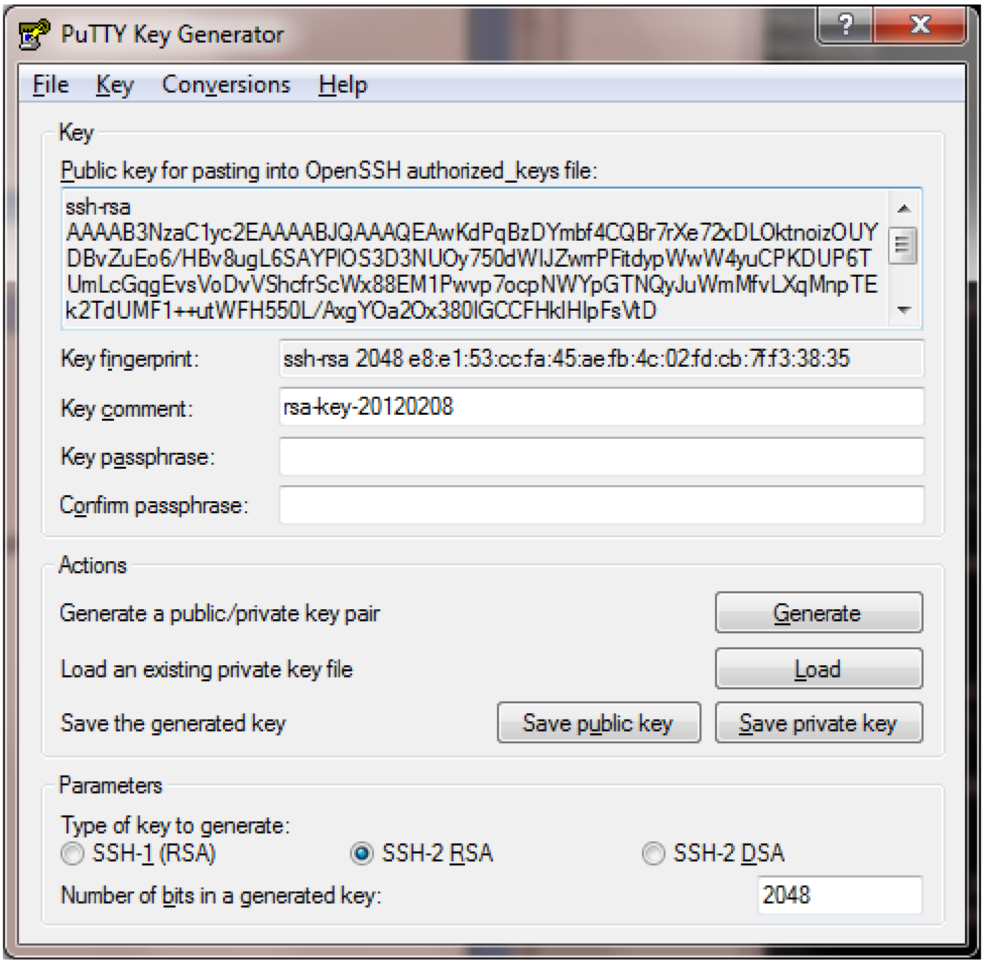
[3] For more information please check https://www.lancom-sytems.de/secureRNG



```
root@:/Setup/Crypto/Rng
> do reseed cdf800bb8186ddfc71899728c530a701bf40bbffa97e188e94bc852cdfca35c205
b7c9b8869ee0a849abc064906909ed
OK: Action reseed done
```

Now, please connect a single trusted host (e.g. notebook) directly to the LANCOM device. Once you connect the RJ45 network cable to one of the free ports of the back of the device, you are able to connect to the LANCOM via TCP/IP. Please make sure your host has an IP-Address within the same network range as used for the device configuration above. In this example, the LANCOM device has the IP-Address 10.10.10.1/24.

Since every LANCOM device initially uses the same SSHv2 RSA-Key (and thus, fingerprint), it is necessary to upload your own unique RSA-Key (fingerprint). You must generate an own SSHv2 RSA Key with a software like PuTTY Key Generator. Please generate an SSHv2 RSA Key with 2048 Bit and make a note of the Key fingerprint shown.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAwKdPqBzDYmbf4CQBr7rXe72xDLOktnoizOUY
DBvZuEo6/HBv8ugL6SAYPlOS3D3NUOy750dWIJZwrrPFitdypWwW4yuCPKDUP6T
UmLcGqgEvsVoDvVShcfrScWx88EM1Pwvp7ocpNWYpGTNQyJuWmMfvLXqMnpTE
k2TdUMF1++utWFH550L/AxgYOa2Ox380IGCCFHkIHlpFsVtD
```

Key fingerprint: ssh-rsa 2048 e8:e1:53:cc:fa:45:ae:fb:4c:02:fd:cb:7f:f3:38:35

Key comment: rsa-key-20120208

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

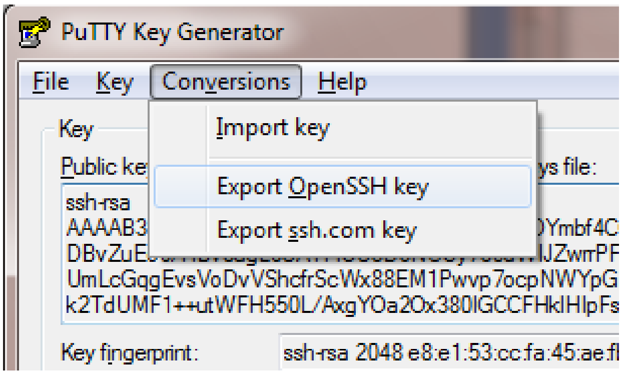
Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

Once generated you must export the SSHv2-RSA-Key and save it as “RSA.key”.



ssh-rsa
AAAAB3)Ymbf4C
DBvZuE JZwrrPF
UmLcGqgEvsVoDvVShcfrScWx88EM1Pwvp7ocpNWYpG
k2TdUMF1++utWFH550L/AxgYOa2Ox380lGCCFHklHlpFs

Key fingerprint: ssh-rsa 2048 e8:e1:53:cc:fa:45:ae:fl

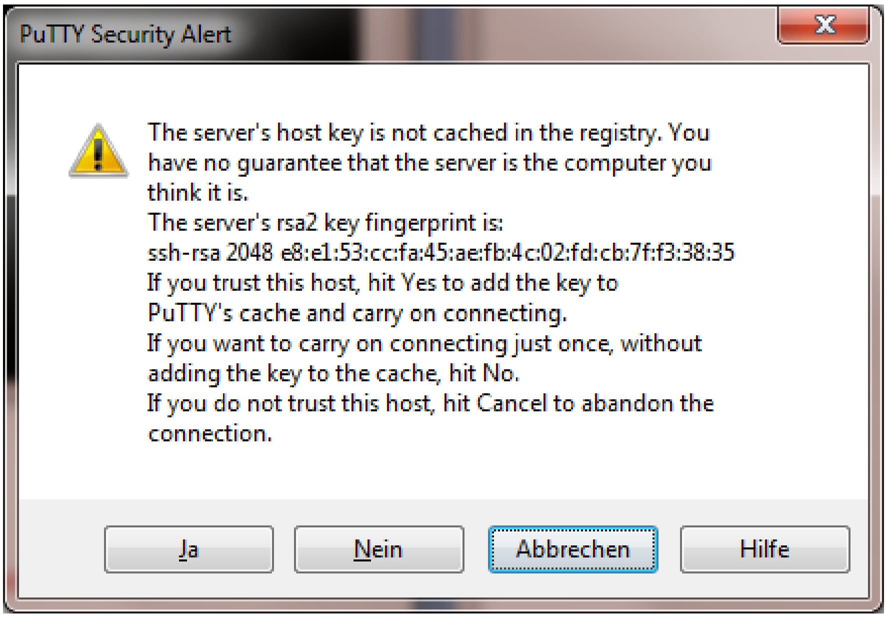
Now you must upload the SSHv2 RSA Key to the LANCOM device. To do this, you must use a secure copy client (e.g. Cygwin SCP or any other management program supporting SCP) in a trusted einvironment. The command to upload the file would be:

- “scp rsa.key root@10.10.10.1:ssh_rsakey”

If you created a key passphrase during the export of the SSHv2 Key, the command would be:

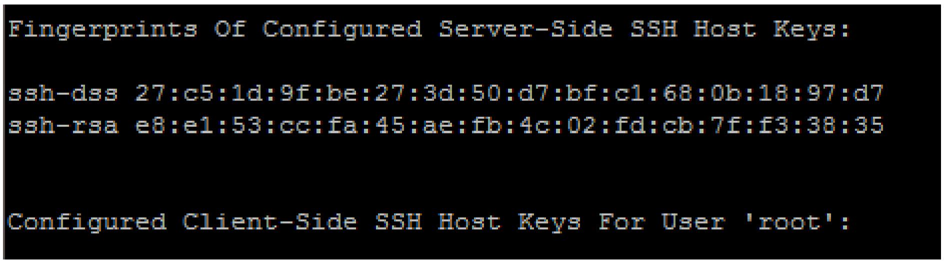
- LCS_PASSWORD=”EnterYourPasswordHere" scp -o SendEnv=LCS_PASSWORD rsa.key root@10.10.10.1:ssh_rsakey

Once uploaded you can login to the LANCOM device via SSHv2 (i.e. PuTTY or any other management program supporting SSHv2) and will probably get an information notification of the new SSHv2 RSA-Key Fingerprint. Please make sure, it has the same fingerprint as noted in the key-generator.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 e8:e1:53:cc:fa:45:ae:fb:4c:02:fd:cb:7f:f3:38:35
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

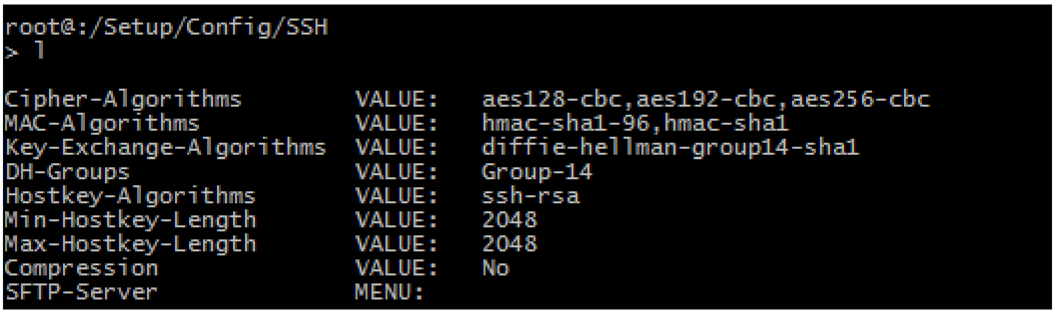
Once logged in, you can also check the RSA-Key Fingerprint by running the command “show ssh”:



```
Fingerprints Of Configured Server-Side SSH Host Keys:

ssh-dss 27:c5:1d:9f:be:27:3d:50:d7:bf:c1:68:0b:18:97:d7
ssh-rsa e8:e1:53:cc:fa:45:ae:fb:4c:02:fd:cb:7f:f3:38:35


Configured Client-Side SSH Host Keys For User 'root':
```

To operate the SSH module in a secure way, only the following parameters are allowed (in /Setup/Config/SSH):

will be checked by cctest



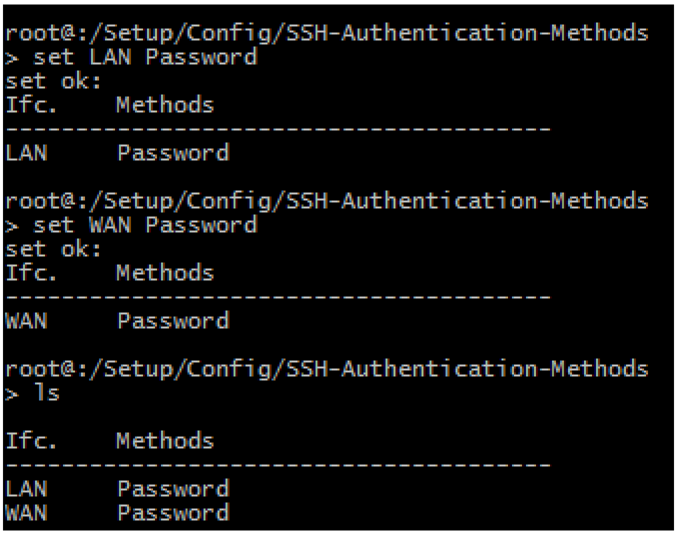
```
root@:/Setup/Config/SSH
> l

Cipher-Algorithms         VALUE:   aes128-cbc,aes192-cbc,aes256-cbc
MAC-Algorithms            VALUE:   hmac-sha1-96,hmac-sha1
Key-Exchange-Algorithms   VALUE:   diffie-hellman-group14-sha1
DH-Groups                 VALUE:   Group-14
Hostkey-Algorithms        VALUE:   ssh-rsa
Min-Hostkey-Length        VALUE:   2048
Max-Hostkey-Length        VALUE:   2048
Compression               VALUE:   No
SFTP-Server               MENU:
```

Cipher-Algorithms:	aes128-cbc, aes192-cbc, aes256-cbc
MAC-Algorithms:	hmac-sha1-96, hmac-sha1
Key-Exchange-Algorithms:	diffie-hellman-group14-sha1
DH-Groups	Group-14
Hostkey-Algorithms:	ssh-rsa
Min-Hostkey-Length:	2048
Max-Hostkey-Length:	2048
Compression	no

It is also necessary to set the SSH authentication method for LAN and WAN to “password” only:

- “set /Setup/Config/SSH-Authentication-Methods/LAN Password”
- “set /Setup/Config/SSH-Authentication-Methods/WAN Password”

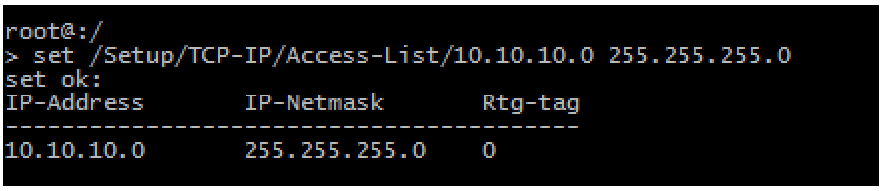
will be checked by cctest



```
root@:/Setup/Config/SSH-Authentication-Methods
> set LAN Password
set ok:
Ifc.     Methods
---------------------------------------
LAN      Password

root@:/Setup/Config/SSH-Authentication-Methods
> set WAN Password
set ok:
Ifc.     Methods
---------------------------------------
WAN      Password

root@:/Setup/Config/SSH-Authentication-Methods
> ls

Ifc.     Methods
---------------------------------------
LAN      Password
WAN      Password
```

The administrator can optionally specify a network or single IP address to limit the remote administration access of the TOE. To only allow the administration from the current local network please type in:

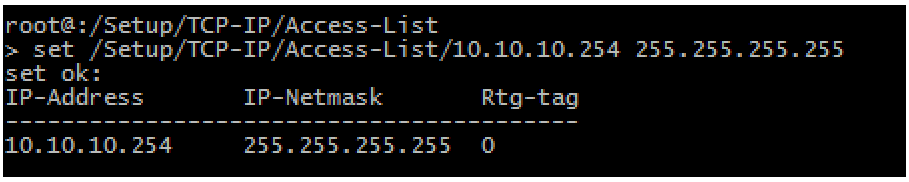
- “set /Setup/TCP-IP/Access-List/10.10.10.0 255.255.255.0”



```
root@:/
> set /Setup/TCP-IP/Access-List/10.10.10.0 255.255.255.0
set ok:
IP-Address        IP-Netmask        Rtg-tag
------------------------------------------
10.10.10.0        255.255.255.0     0
```

If you only wish to allow one single IP address (e.g. 10.10.10.254) the command would be:

- “set /Setup/TCP-IP/Access-List/10.10.10.254 255.255.255.255”

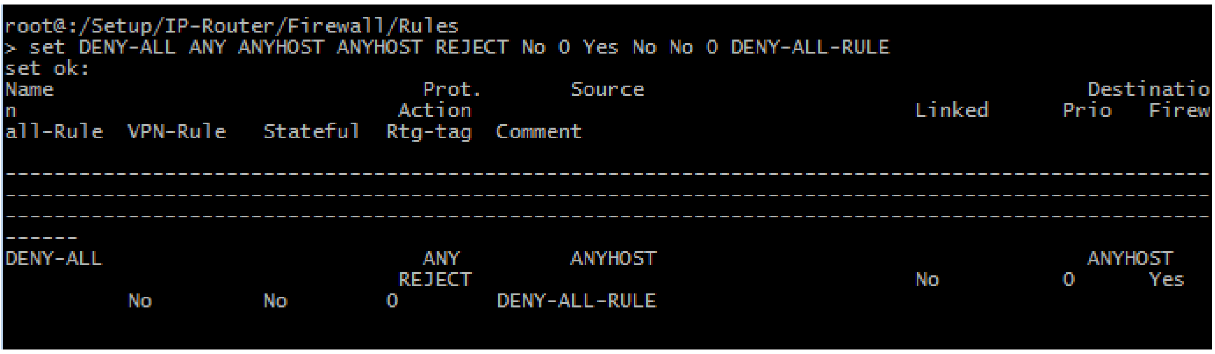


```
root@:/Setup/TCP-IP/Access-List
> set /Setup/TCP-IP/Access-List/10.10.10.254 255.255.255.255
set ok:
IP-Address        IP-Netmask        Rtg-tag
------------------------------------------
10.10.10.254      255.255.255.255   0
```

The last step is to configure the internal firewall. When configuring the firewall, you must create a deny-all rule (deny-all strategy) at first. This must be done in /Setup/IP-Router/Firewall/Rules

A possible command might be:

“set DENY-ALL ANY ANYHOST ANYHOST REJECT No 0 Yes No No 0 DENY-ALL-RULE”



```
root@:/Setup/IP-Router/Firewall/Rules
> set DENY-ALL ANY ANYHOST ANYHOST REJECT No 0 Yes No No 0 DENY-ALL-RULE
set ok:
Name                                  Prot.        Source                                          Destinatio
n                                   Action                                           Linked       Prio    Firew
all-Rule  VPN-Rule   Stateful  Rtg-tag  Comment

----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
------
DENY-ALL                              ANY          ANYHOST                                         ANYHOST
                                    REJECT                                           No           0       Yes
          No         No         0         DENY-ALL-RULE
```

With this step the initial setup is finished. The device must now be configured further as described in the operative user guidance documentation and be connected to the networks.

1.2.4. Startup of the TOE

The previous configuration settings will not be affected by a restart of the TOE. Thus the administrator is not required to perform an action after a restart.

1.3. Identification of the TOE

The Target of Evaluation (TOE) is called LANCOM Systems Operating System LCOS 8.70 CC with IPsec VPN.

No.	Type	Identifier	Release	Form of Delivery
1	Software	LCOS 8.70 CC	8.70 CC	Firmware is downloadable at the end of the certification process at https://www.lancom.de/cc

The certification report will contain a SHA-256 hash of the firmware file. The user must ensure the downloaded firmware is genuine as described in section 1.1 (Acceptance Procedures).