



How to recover Cisco 7961 with SCCP

created by: Rainer Bemsel - Version 1.0 - Dated: NOV/19/2011

The purpose of this document is to provide a set of instructions about how to recover a Cisco phone and load SCCP Software. You do not need to have a Cisco Call Manager to run the recovery process.

There are several entries in different forums about that topic, but all I've consulted seem to miss a piece of the whole challenge.

First of all, you need to be very patient during that process. Even you think the phone is "dead". In Reality, the phone is requesting DHCP Address (if not set to permanent) followed by TFTP File requests.

STEP 1: Download the Cisco Phone Firmware

Go to www.cisco.com/go/software and find the right phone firmware. You will need to have a support contract before you can download the firmware. There are other resources on the internet where you can get those files as well.

The screenshot shows the Cisco Download Software page for the Cisco Unified IP Phone 7961G. It includes a breadcrumb trail: > Products > Voice and Unified Communications > IP Telephony > IP Phones > Cisco Unified IP Phone 7900 Series > Cisco Unified IP Phone 7961G. Below the breadcrumb, there are links for Configuration Assistant Software, Session Initiation Protocol (SIP) Software, Skinny Client Control Protocol (SCCP) Software, and Unified Communications Manager Endpoints Locale Installer. On the right, there are buttons for 'Download Now' and 'Add to cart', and a summary of the download: cmterm-7941_7961-sccp.8-3-3.zip, Release Date: 23/OCT/2007, 7941/7961 SCCP IP Phone firmware files only - Compatible CUCM Versions: 3.3, 4.0, 4.1, 4.2, Size: 4136.94 KB (4236224 bytes).

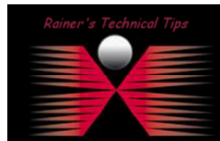
I was using 8.3 (3) to have a compatible version for upgrading with my Cisco Call Manager 8.x after registration. There is another TechTip telling about that issue "Authentication Fail when register with CUCM"

Make sure you download the zip-file, as this is the best choice to upgrade outside of Call Manager.

The screenshot shows the IZArc file manager window displaying the contents of the file cmterm-7941_7961-sccp.8-3-3.zip. The file list includes:

File Name	File Type	Modified	Size	Ratio	Packed	CRC
apps41.8-3-2-27.sbn	SBN File	10/19/2007 9:09:16 AM	2,494,499	65%	866,141	C1126C4E
cnu41.8-3-2-27.sbn	SBN File	10/19/2007 9:09:14 AM	547,146	10%	490,856	8B9A45F3
cvm41sccp.8-3-2-27.sbn	SBN File	10/19/2007 9:09:20 AM	2,452,629	1%	2,438,447	84AA0500
dsp41.8-3-2-27.sbn	SBN File	10/19/2007 9:09:18 AM	530,601	61%	207,119	81263E7C
jar41sccp.8-3-2-27.sbn	SBN File	10/19/2007 9:09:18 AM	315,827	27%	231,088	C66EA2B4
SCCP41.8-3-3S.loads	LOADS File	10/19/2007 9:09:08 AM	638	15%	540	AAE52753
term41.default.loads	LOADS File	10/19/2007 9:09:10 AM	642	15%	543	2B8124B2
term61.default.loads	LOADS File	10/19/2007 9:09:12 AM	642	15%	544	2765F886

Summary: Type: ZIP, Files: 8, Packed: 4,235,278, Unpacked: 6,342,624, Ratio: 33%



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user.

STEP 2: Prepare your PC or Laptop to support the Upgrade

Freeware Tools, I have used:

- a) TFTP Server to provide the firmware loads
<http://tftpd32.jounin.net/>

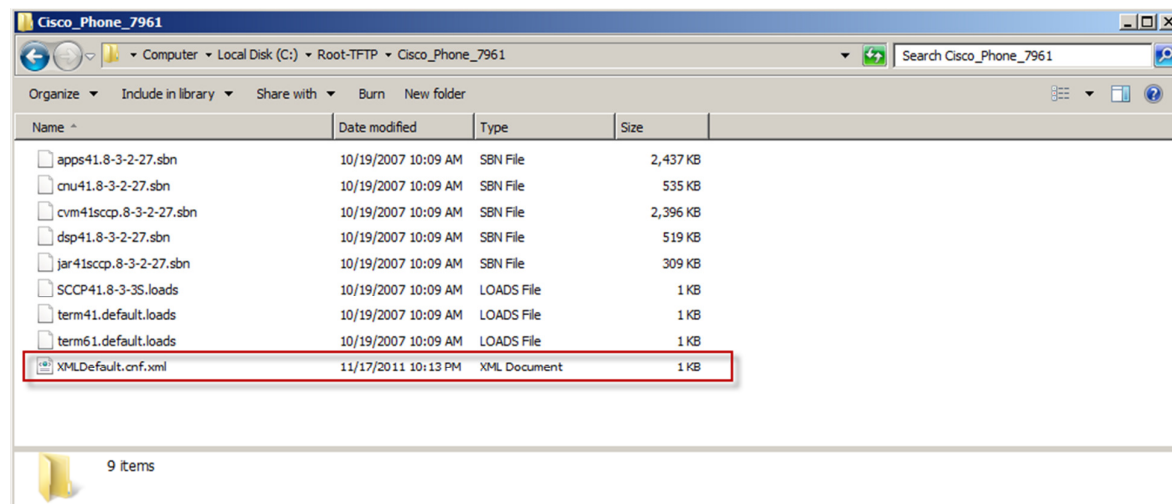
1st June 2007	v3.23	tftpd32.323.zip (444 kB) tftpd32-3.23-setup.exe (480 kB)
---------------	-------	---

Note: This version seems to be best fit and most likely smart and smooth working

- b) WinDump to see packets coming in
<http://www.winpcap.org/windump/default.htm>
- c) Observer (not a freeware) or Wireshark to packet analyze firmware load
<http://www.networkinstruments.com/products/observer/expert.html>

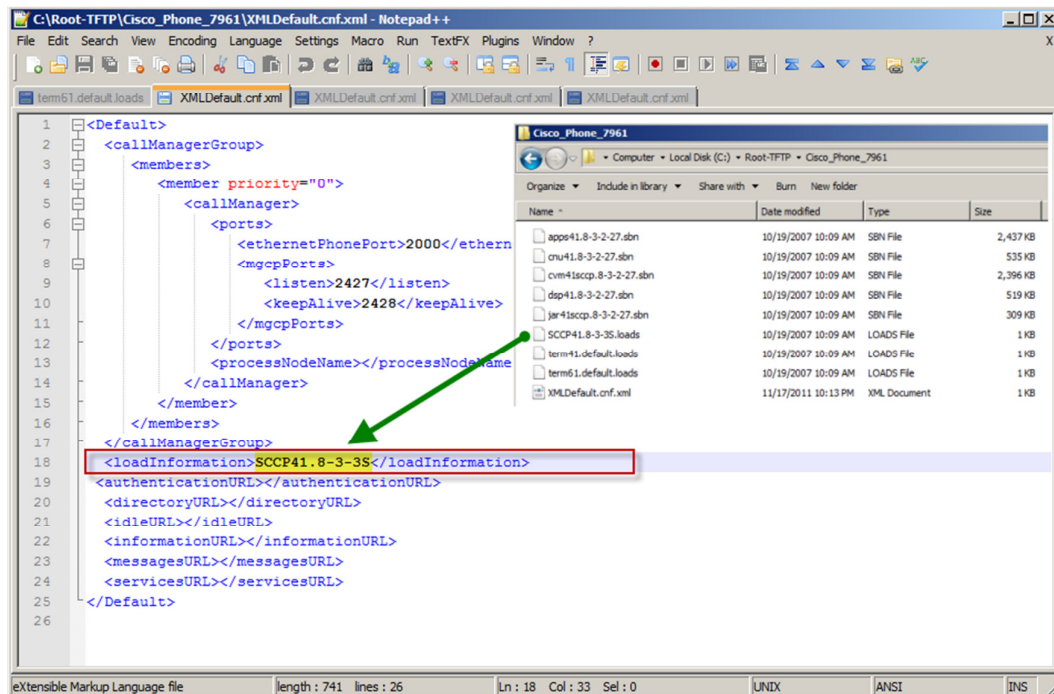
STEP 3: Install TFTP Server and make adjustments

The installation is simple forward. Just run the executable. After installation, place the extracted files in the upload directory of your choice.

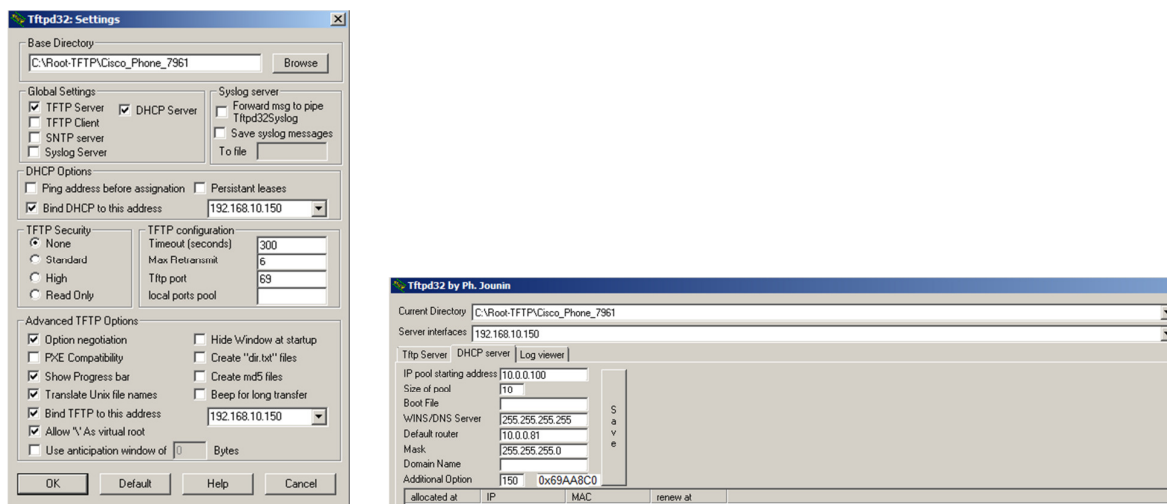


XMLDefault.cnf.xml is not part of the Firmware Package.

You need create a new file or download from here: <http://www.bemsel.com/tools/HelpFiles/XMLDefault.cnf.xml>

STEP 4: Create Default XML File and configure for proper firmware load

The **loadInformation** needs to be exactly the LOADS file from your firmware tftp upload directory

STEP 5: Configure DHCP Server if required

DHCP Option 150 - see also next page

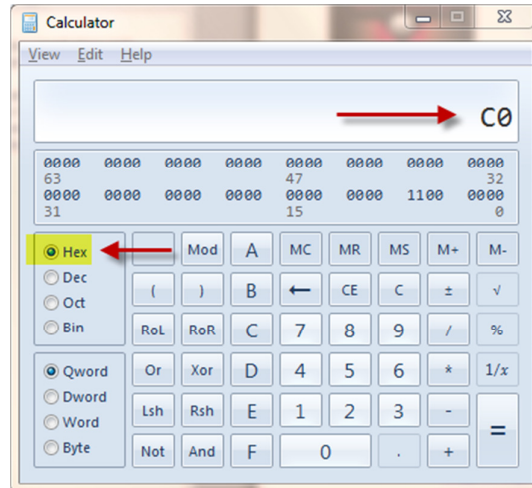
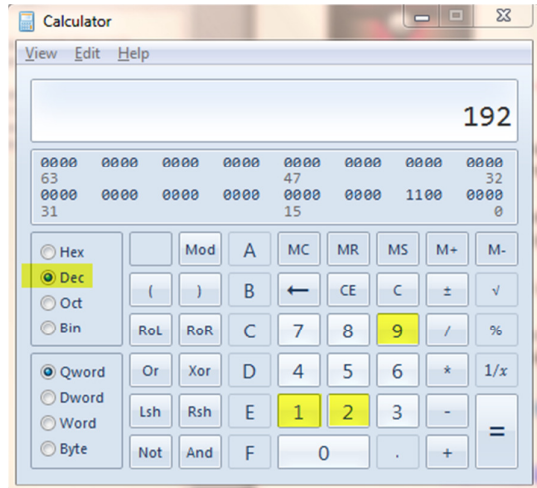
<http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xml>

Cisco Phone to load SCCP required TFTP Server Address; this is what Option 150 provides for DHCP Requests. This needs to be provided by HEX in Reverse

You can use the Programmer Calculator of Windows, or any other online tool. All you need to do is to convert each Byte of the IP Address and put in reverse into the option value

192.168.10.105 -> 105.10.168.192 -> 0x69AA8C0

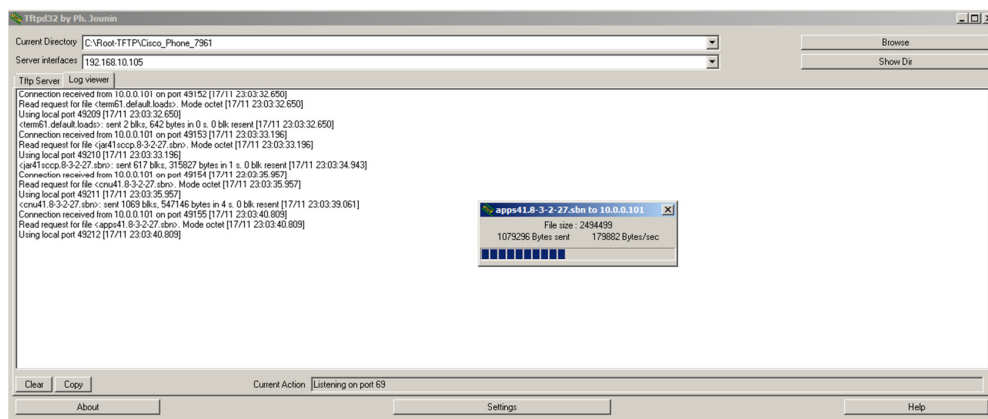
192.168.1.1 -> 1.1.168.192 -> 0x0101A8C0



STEP 6: Reset Cisco Phone 7961

1. Pull power on the phone (even if power is PoE).
2. Hold down the # key on the phone.
3. Continue holding down the # key and re-apply power
4. While still holding the # key wait for the Message Waiting Indicator (MWI) light on the handset to start flashing amber.
5. Once the MWI light is flashing amber, release the # key and enter the following sequence exactly on the keypad: 3491672850*#
6. The amber lights are turning red. That's when the phone deletes configuration and firmware.
7. It will reboot and tries to get an IP Address via DHCP. Option 150 does the Auto-Provision the TFTP Server IP Address

For more DHCP options: <http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xml>



A few troubleshooting points.

Once this sequence has been entered on the IP Phone, if all the network criteria above have been met, it should begin its recovery process. This process can take up to 15 minutes to finish. The phone may appear to be doing nothing during this time. However, if the phone does not recover after 20 minutes then it is possible that the recovery is stuck. In this case, re-examine your network and verify that steps 1-4 are in place, and then re-issue the factory reset sequence.

During my troubleshooting experience, I spanned the Phone Port to a packet analyzer to see what's going on the wire.

7	192.168.10.105	10.0.0.101	65	11/18/2011 10h:02m 35.540 4...	0.001 319	09.768380	TFTP Error [5] ---- UDP [33138 -> 49153] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
8	10.0.0.101	192.168.10.105	73	11/18/2011 10h:02m 35.619 0...	0.078 553	09.846933	TFTP Read request [1] ---- UDP [49154 -> 69] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
9	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.621 6...	0.002 652	09.849585	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
10	10.0.0.101	192.168.10.105	68	11/18/2011 10h:02m 35.621 6...	0.000 006	09.849591	TFTP Ack [4] ---- UDP [49154 -> 33138] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
11	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.623 0...	0.001 322	09.850913	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
12	10.0.0.101	192.168.10.105	68	11/18/2011 10h:02m 35.624 3...	0.001 332	09.852245	TFTP Ack [4] ---- UDP [49154 -> 33138] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
13	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.625 6...	0.001 331	09.853576	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
14	10.0.0.101	192.168.10.105	68	11/18/2011 10h:02m 35.627 0...	0.001 331	09.854907	TFTP Ack [4] ---- UDP [49154 -> 33138] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
15	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.628 3...	0.001 332	09.856239	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
16	10.0.0.101	192.168.10.105	68	11/18/2011 10h:02m 35.629 6...	0.001 332	09.857570	TFTP Ack [4] ---- UDP [49154 -> 33138] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
17	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.630 9...	0.001 330	09.858901	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE
18	10.0.0.101	192.168.10.105	68	11/18/2011 10h:02m 35.632 3...	0.001 331	09.860232	TFTP Ack [4] ---- UDP [49154 -> 33138] ---- IP [10.0.0.101 -> 192.168.10.105] ---- ETHERTYPE
19	192.168.10.105	10.0.0.101	562	11/18/2011 10h:02m 35.633 6...	0.001 332	09.861564	TFTP Data [3] ---- UDP [33138 -> 49154] ---- IP [192.168.10.105 -> 10.0.0.101] ---- ETHERTYPE

p8: 10.0.0.101 -> 192.168.10.105	
IP: 10.0.0.101 -> 192.168.10.105	
UDP, [49154] TFTP -> [69]	
Source port	[49154]
Destination port	[69]
UDP length	35
Checksum	0x0000 (not used)
TFTP Section: 27 bytes	
Opcode	1: Read request
Filename	>XMLDefault.cnf.xml
Mode	octet

Remember the XMLDefault.cnf.xml file, you modified in Step 4.

Don't be afraid to re-run that procedure in the case, if you think it didn't finished successfully. I did it several times in the first place.

Note: The factory reset sequence is a way for a phone to clear flash and still upload to a valid firmware image. This is facilitated by the termxx.default.loads file, but requires that the image files listed in the termxx.default.loads file are available in TFTP for the phone to download. Open the termxx.default.loads file in any text editor. This loads file is essentially just a packing list showing all the OS and application files the phone needs to function. The files include a cnu, cvm, dsp, app and jar files. Please make sure that these files as listed in the termxx.default.loads file are in TFTP. ("xx" will be either "41" for the CP-7941 model, or "61" for the CP-7961 model.)