TelePresence

Troubleshooting TelePresence with Mac Tips and Tricks

Copyright © 2012 Cisco Systems, Inc.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Troubleshooting TelePresence with Mac Tips and Tricks
September 2012 Edition
© 2012 Cisco Systems, Inc. All rights reserved.

Table of Contents

List of Tables

Copyright © 2012 Cisco Systems, Inc.

1 Introduction

This guide is an introduction on how to use a MAC for common TelePresence troubleshooing tasks and how they can be done vs on a Windows machine

1.1 Release Notes

Table 1 - Release Notes

Technical Change	Title(s) of Affected Section(s)	Changes Made By	Date
Initial Release		Matt Limbrick	9/25/2012

2 Using a Serial Port

Because many laptops no longer come with serial ports as a standard, most of the time you can find a compatible USB to serial adapter for Mac.

(Future Technology Devices USB Serial Converter)

3 Viewing the USB Connected to Your Mac

To view the USB connected to your Mac:

1. Open the terminal.
2. With the USB to Serial adapter (Future Technology Devices USB Serial Converter) plugged into the MAC, enter the following command to see all connected device: ***ls /dev***
3. Although you see a lot of entries, look for: **tty.usbserial-“Model of USB”** (i.e., tty.usbserial-FTDGDWLU)

Copyright © 2012 Cisco Systems, Inc.

4. To get the statistics of the device, type: `stty -f /dev/tty.usbserial-FTDGDWLU`
   The following is an example of the output:
   ```
   :~ mlimbric$ stty -f /dev/tty.usbserial-FTDGDWLU
   speed 9600 baud;
   lflags: -icanon -isig -iexten -echo
   iflags: -icrnl -ixon -ixany -imaxbel -brkint
   oflags: -opost -onlcr -oxtabs
   cflags: cs8 -parenb
   ```
5. After you know the device you have connected to your system, you can open a new connection session with that device by typing the following command, where 38400 is the baud rate:
   ```
   screen /dev/tty.usbserial-FTDGDWLU 38400
   ```

In addition, there are other serial port terminal applications available for Mac, such as CoolTerm, ZTerm and goSerial.

4 SSH & Telnet

(The scenarios below are demonstrated while connecting to a 1700MXP)

Fortunate enough for Mac users, SSH and Telnet are native to Mac.

4.1 Using Telnet:

Open Terminal

Type: `telnet “IP address of node”` (i.e., `telnet 10.83.23.247`)

The following are the results:

```
:~ mlimbric$ telnet 10.83.23.247
Trying 10.83.23.247...
Connected to 10.83.23.247.
Escape character is '^]'.
Welcome to 1700MXP-1 Lab
TANDBERG Codec Release F9.1.2.1 NTSC
SW Release Date: 2012-06-08
OK
```

If a password is required, you are prompted for a username and password before the connection completes.

4.2 Using SSH:

Open Terminal
Type: `ssh username@“IP address of node”` (i.e., `ssh admin@10.83.23.247`)

The following are the results:

```
:~ mlimbric$ ssh admin@10.83.23.247
The authenticity of host '10.83.23.247 (10.83.23.247)' can't be established.
DSA key fingerprint is e5:6a:4e:59:fc:95:86:d7:65:53:18:8f:37:98:fe:e5.
Are you sure you want to continue connecting (yes/no)? yes
```

Copyright © 2012 Cisco Systems, Inc.

NOTE: Upon 1st connection of your Mac to a new device via SSH, you are prompted to continue adding this device connection to a list of known hosts. After you approve, you are prompted for a password if one is required to access the device. This connection is saved in a host file and you should not be prompted again to add it.

Continuation of the results:

```
Warning: Permanently added '10.83.23.247' (DSA) to the list of known hosts.
admin@10.83.23.247's password:
```

NOTE: Once the password has been accepted and you have authenticated, you will be given access to the CLI

Continuation of the results:

```
Welcome to 1700MXP-1 Lab
TANDBERG Codec Release F9.1.2.1 NTSC
SW Release Date: 2012-06-08
OK
```

4.2.1 SSH Host File Editing:

If you attempt to SSH into an IP address (i.e.192.168.1.2) where the hostname associated to it has changed, you see the following error and arenot be able to connect:

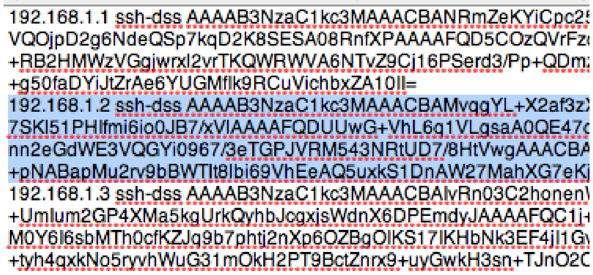
```
@@@@@@@@@@@@@@@@@@@@@@@@@@
@ REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
----------------------------------------------------
Please contact your system administrator.
Add correct host key in /Users/user/.ssh/known_hosts to get rid of this message.
Offending key in /Users/user/.ssh/known_hosts:6
RSA host key for 10.1.1.50 has changed and you have requested strict checking.
Host key verification failed.
```

NOTE: To fix this issue, you need to remove the whole entry associated with the IP address you are attempting to access. Use the following command:

Open /Users/"user logged in"/.ssh/known_hosts (i.e. open /users/mlimbric/.ssh/known_hosts)

This opens "known_hosts" in TextEdit. This is your host file where you will need to locate the IP address (of the device you are attempting to connect) on the left. Select all the text from the beginning of the IP (*192.168.1.2*) to the next IP address and delete it. Save and close the file.

Copyright © 2012 Cisco Systems, Inc.



```
192.168.1.1 ssh-dss AAAAB3NzaC1kc3MAAACBANRmZeKYiCpc2
VQOjpD2g6NdeQSp7kqD2K8SESA08RnfXPAAAAFQD5COzQVrFz
+RB2HMWzVGgjwrxl2vrTKQWRWVA6NTvZ9Cj16PSerd3/Pp+QDm
+g50faDYiJtZrAe6YUGMflk9RCuVichbxZA10Il=
192.168.1.2 ssh-dss AAAAB3NzaC1kc3MAAACBAMvqgYL+X2af3z
7SKl51PHlfmi6io0JB7/xVlAAAAFQDUUwG+VhL6q1VLgsaA0QE47
nn2eGdWE3VQGYi0967/3eTGPJVRM543NRtUD7/8HtVwgAAACB
+pNABapMu2rv9bBWTIt8lbi69VhEeAQ5uxkS1DnAW27MahXG7eK
192.168.1.3 ssh-dss AAAAB3NzaC1kc3MAAACBAlvRn03C2honen
+Umlum2GP4XMa5kqUrkQyhbJcqxjsWdnX6DPEmdyJAAAAFQC1j
M0Y6l6sbMTh0cfKZJq9b7phtj2nXp6OZBgOlKS17lKHbNk3EF4jl1G
+tyh4qxkNo5ryvhWuG31mOkH2PT9BctZnrx9+uyGwkH3sn+TJnO2
```

Reconnect to the IP again via SSH. This time, you are prompted again to re-add this device connection back to your host file as a new entry. Approve and authenticate as needed.

5 SCP Protocol

Unfortunately, the ever-popular WinSCP application for Windows is not available for Mac. However, SCP is also native to Mac, but if you really must use WinSCP, you can run a Windows Virtual Machine (VM) using VMware Fusion, Parallels or Virtual Box (free), not covered in this guide.

5.1 To run native SCP on Mac:

1. Open terminal
2. Type "`scp root@IPofDevice:`
3. Type the path of the file after the ":"
4. "~/documents" copies the file from the remote device to the document folder of the user currently logged onto the MAC.

   Command Syntax:
   scp username@"ip of device":"path of source" "path of destination"

5) If prompted, enter the a password for the username

Complete syntax example:

scp root@10.83.23.45:/mnt/harddisk/traces/trace.pcap ~/documents (***for a single file)***
Produces the following output:

```
Last login: Tue Sep 18 12:35:34 on ttys000
:~ mlimbric$ scp root@10.83.23.45:/mnt/harddisk/traces/trace.pcap ~/documents
VCS VM Mlimbric
VCS VM Mlimbric

Password:
trace.pcap                              100% 1114     1.1KB/s   00:00
:~ mlimbric$
```

scp -r root@10.83.23.30:/tandberg/log ~/documents **(Use "-r" a complete directory**)
Produces the following output:

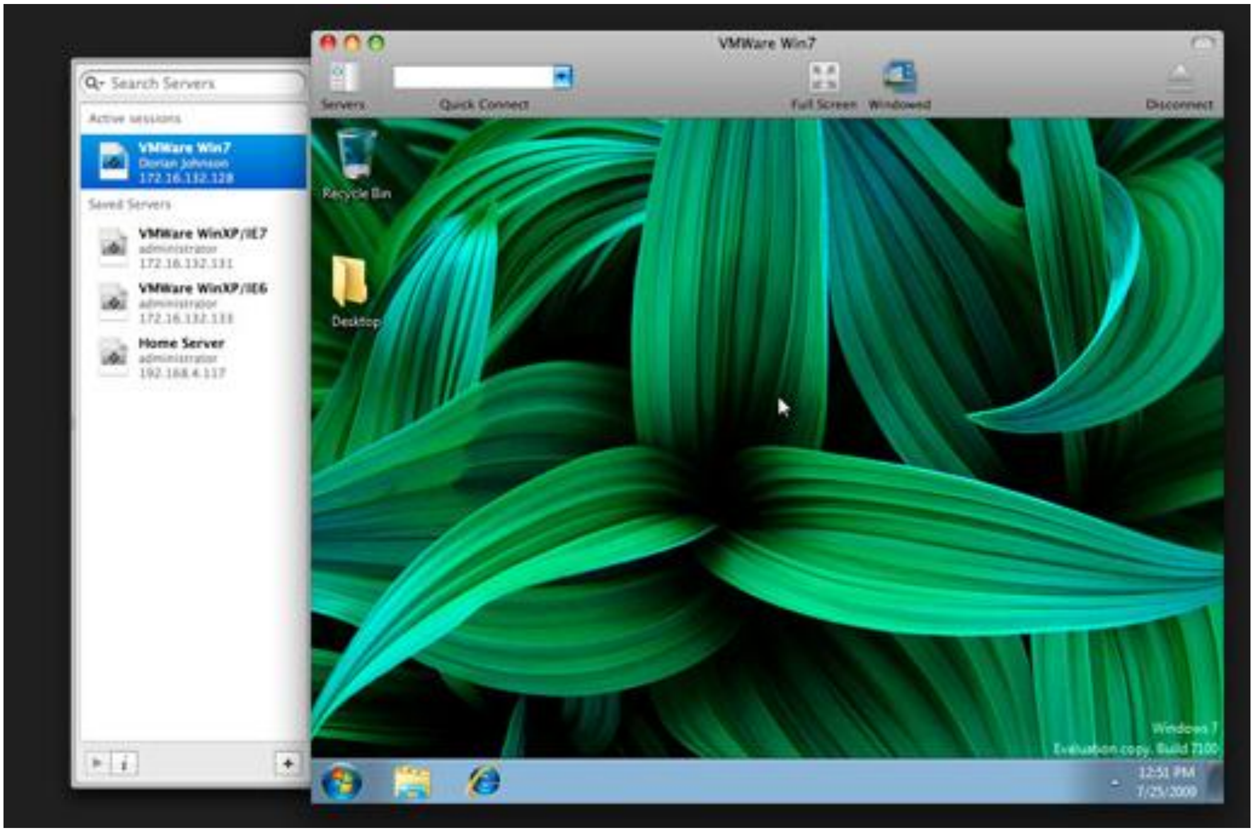
```
dhcp-10-150-1-227:~ mlimbric$ scp -r root@10.83.23.45:/mnt/harddisk/traces/ ~/documents
VCS VM Wilhoang
VCS VM Wilhoang
```

Copyright © 2012 Cisco Systems, Inc.

```
Password:
trace2.pcap                          100% 1149     1.1KB/s   00:00
trace.pcap                          100% 1114     1.1KB/s   00:00
dhcp-10-150-1-227:~ mlimbric$
```

6 Remote Desktop:

Preferably use "**CoRD**" as the default RDP client, but you can use others including "**Microsoft Remote Desktop Connection Client for MAC**". **CoRD** has an easier to use interface that lists all your saved connections directly on the main Window



Download CoRD from http://cord.sourceforge.net/

7 Network Tools:

All the standard CLI network commands are available in "**Terminal**". You can also use the native "**Network Utility**" application. Other applications are available to download such as "**Angry IP scanner**" to scan a group of IP addresses at one time. "**Wireshark**" also has a version available on Mac. "**Cyber Duck**" is an FTP GUI client that is easy to use.

8 Text Editors:

"**TextWrangler**" is a handy application for reading log files and text edits if you choose not to use native "**TextEdit**" or "**Console.**"

Copyright © 2012 Cisco Systems, Inc.

End of Document

Copyright © 2012 Cisco Systems, Inc.