Your Step-By-Step Guide For:

Gathering Field Debug Information

96x1 H323/SIP Series

Author: Eli Shmulenson

Last update: April 2016
Doc Version: 20.3

1 Introduction:

1.1. The purpose of this document is to be used as a handy guiding tool for collecting debug info, valid for the Avaya 96x1 series desk phones: 9608, 9608G, 9611G, 9621, 9641, 9641GS.

1.2. This guide enables a fast drill-down from the main menu to all details via internal hyperlinks.

1.3. This guide doesn't deal with an on-site debugging, but only with gathering information.

1.4. Please make sure to work with a guidance document version which fits the actual SW version.

1.5. For short and quick reporting go to phone report via menu and description sections only.

1.6. Some functions require installation and activation of debug capable authentication file. This document doesn’t cover this topic.

USE HYPERLINKS TO NAVIGATE

2 Main Menu

The following 6 items are the full list of the general types of information required by R&D.
Please go over each item and its sub-items and try to collect the most relevant information.
For further field information, R&D will provide specific guidance.

3 Debug Reports

- Phone Report
- Crash Report
- Audio report

Press **Alt + Left Arrow** to return back to previous view

3.1 Phone Report

This report can be generated any time, per user request, and it includes information regarding the phone last events and a "snapshot" of registers and parameters values. The report can be simply opened by Winzip (tgz file) and includes standard viewable text files inside.
Generating and extracting the phone report can be done by two ways:

1. Via phone menu (not possible during a call)
2. Via shell

Press **Alt + Left Arrow** to return back to previous view

3.1.1 Phone Report via phone menu (H323 sets only)

1. Press "Mute", 'C', 'R', 'A', 'F', 'T', '#'
2. Scroll down and select "DEBUG" (See "Why DEBUG option doesn't appear" in section 11)
3. Make sure "Log to File" is On. Otherwise set it to On (see section 5.5)
4. Select "Phone Report"
5. The report file (named: [ext]_report.tgz) will be uploaded to the http location mentioned in BRURI parameter at the settings file (backup/restore server).
6. Press "Exit"

Note: When there is no BRURI parameter in the settings file, the menu will display "Create" instead of "Send" and the report will be saved in the RAM, and can be collected via shell.

Press **Alt + Left Arrow** to return back to previous view

3.1.2 Phone Report (Via shell)

1. Open shell as user “craft”.

2. Run the following command, based on the phone type being used:

For 96x1 H323 phones with P/N 700511225 and 700511227, run the command:

```
/AvayaStatic/bin/phone-report
```

For other 96x1 H323 phones P/Ns, run the command:

```
/AvayaDir/lib/phone-report
```

For 96x1 SIP phones with P/N 700511225 and 700511227, run the command:

```
/AvayaStatic/bin/phone-report-user
```

For other 96x1 SIP phones P/Ns, run the command:

```
/AvayaDir/lib/phone-report-user
```

3. This will generate the phone report at folder **/tmp** or **/var/log** (for SIP root users).

The report name is “phone_report.tar.gz” or “phone_report_craft.tar.gz” (for craft users).

4. Upload the output file to the PC or copy it to a USB device.

Press **Alt** + **Left Arrow** to return back to previous view 4

3.2 Crash Report

This is a partial phone report which is generated automatically by watchdog during crash.
In order to provide a full crash report, the following items should be included:

3.2.1 Crash information files

The crash information is saved at: /var/log/wd_crash.[num].gz and includes various system parameters.

Note: This part of the crash report is also included in the phone report.

3.2.2 Crash core files

Crash core files are not included in phone report and should be uploaded separately:

Extracting steps:

1. Open shell.

2. Check via shell whether core files (.core) are available in **/data/crash** or **/var/crash** (depends on the phone type). You can use the "`ls -al`" command to look for an existing .core file in the above directories.

3. Optional: compress cores before uploading: gzip [core filename].core

4. Please don't change core files names, as it contains valuable information.

5. Upload the output file to the PC or copy it to a USB device.

Press **Alt + Left Arrow** to return back to previous view

3.3 Audio Report (H323 sets only)

This report includes the full phone report and additional audio information.
Available only when "AUDIOREPORT" is set to "1" in the settings file.
Creation and extraction steps:

1. Verify via the phone menu that the "Logging Mode" is "On". Otherwise, Set it to "On".
Logging may be enabled also on multiple phones via settings file by: SET LOGTOFILE 1

Note: When Logging mode is OFF, the audio report will include only partial information.

2. Press "Home" (A-Menu) or select "Settings" in touch phones

3. Select "Network Information" and then select "Report" Soft Key

4. The output is generated at: /tmp/Audio_Report.tar.gz

5. Generate a Phone Report through the menu. This will upload the Audio Report to the BRURI server together with the Phone Report.

Note: You might experience slow responsiveness when accessing the phone during report collection.

6. If you don't have BRURI configured then you can upload the output file to the PC or copy it to a USB device.

It is also possible to generate an Audio Report through the shell:

For 96x1 H323 phones with P/N 700511225 and 700511227, run the command:

```
/AvayaStatic/bin/phone-report -a
```

For other 96x1 H323 phones, run the following command:

```
/AvayaDir/lib/phone-report -a
```

The output will be generated at /tmp/Audio_Report.tar.gz.

4 Network Captures

1. Record a capture (Wireshark) of the relevant scenario.

2. In case an external switch or a hub isn't available for mirroring, use the secondary socket of the phone (PC port) for phone-internal mirroring.

3. In case of any other problem (no eth cable, no capturing tools), or in case R&D needs a capture directly from within the operating system, use TCP Dump.

4. For on-the-fly L2 traffic monitoring read the switch counters table (see section 4.3).

5. For on-the-fly IP-MAC table read the switch CAM table (see section 4.4).

Notes:

1. Please verify that VLAN values are included (sometimes they are removed by the network card during capturing). For further information please visit: https://wiki.wireshark.org/CaptureSetup/VLAN

2. To see H323 packets (not required) use Avayashark instead of Wireshark.

3. If TLS is being used, then most of the Wireshark trace will be unreadable. To trace the messaging between the SIP endpoint and the server, enable SIPMESSAGE syslogs at the debug level.

Press **Alt + Left Arrow** to return back to previous view

4.1 Phone internal mirroring

The phone internal switch has 3 active ports: LAN, PC and CPU (internal port).
After performing the below steps, all ingress and egress traffic of the LAN port will be copied to the PC port. Packets which are already targeted to the PC port, won't be duplicated.

Mirroring will be disabled after hard restart.

Activating the port mirroring may be done in two ways:

- Via phone menu (applicable for H323 phones only)
- Via shell (applicable for both H323 and SIP phones)

Press **Alt + Left Arrow** to return back to previous view

4.1.1 Mirroring via phone menu (H323 sets only)

This phone menu capability is supported from 6.2 SP2 and on for H323 endpoints.

1. Press “Mute”, ‘C’, ‘R’, ’A’, ’F’, ’T’, ‘#’
2. Scroll down and select “DEBUG” (See “Why DEBUG” option doesn’t appear” in section 11)
3. Change “Port Mirroring” to “On”
4. Press “Save”
5. Press “Exit”

The above action will not reboot the phone and no reboot is required.

4.1.2 Mirroring via shell (for both SIP and H323)

Note: This procedure requires privileged shell access.

Port mirroring via shell is supported from release 6.0 for both SIP and H323.

1. Open shell
2. Login as user “root” by running the command: `su -`

Note: Root level access is disabled by default. To enable root level access a debug capable authentication file with root access support has to be installed and activated on the phone (this procedure is out of scope of this document).

3. For 96x1 H323 phones with P/N 700511225 and 700511227, run the following commands:

```
rtl1836nb_cli
CLI> set_port_mirror 2 1
CLI> q
```

For other 96x1 phones, run the following commands:

```
eth mir toport 0
eth mir ingr port 1 1
eth mir ingr filter all
eth mir egr port 1 1
eth mir egr filter all
eth mir en 1
```

Press **Alt + Left Arrow** to return back to previous view

4.2 TCP Dump Trace

Note: This procedure requires privileged shell access.

This capability enables a capturing of a PCAP trace file from within the phone, locating it on the phone RAM for later uploading.

1. Type the following command from shell:

```
tcpdump -s 0 -w /tmp/test.pcap &
```

2. Run the relevant scenario which you wish to capture.
3. Stop the tcpdump process by:

```
ps -x | grep tcpdump
kill -9 [tcpdump process ID]
```

(to see the process ID as the first number on the left)

4. Upload the output file (/tmp/test.pcap) to the PC or copy it to a USB device.

Tcpdump also supports a rotating window capturing. The following example creates an overwritten sliding window of 4 files with 5 million bytes per file:

```
tcpdump -s 0 -W 4 -C 5 -w /tmp/test.pcap
```

Press **Alt + Left Arrow** to return back to previous view 7

4.3 Switch Counters Table

Note: This procedure requires privileged shell access.

To read the counters of the internal switch type the following command from shell.

1. Open shell
2. Login as user “root” by running the command: `su -`

Note: Root level access is disabled by default. To enable root level access a debug capable authentication file with root access support has to be installed and activated on the phone (this procedure is out of scope of this document).

3. For 96x1 H323 phones with P/N 700511225 and 700511227, run the following commands:

```
rtl1836nb_cli
CLI> show_counters 7
CLI> show_port_status
CLI> show_port_priority_pvid
```

(Where: PC port is #1, LAN port is #2 and CPU port is #4)

For other 96x1 phones run the following commands:

```
eth mib show
```

To clear the counters use:

```
eth mib clr
```

(Where: PC port is #0, LAN port is #1 and CPU port is #8)

Press **Alt + Left** Arrow to return back to previous view

4.4 Switch CAM Table

Note: This procedure requires privileged shell access.

To read the internal ports status and the CAM table of the internal switch type the following command from shell.

1. Open shell
2. Login as user "root" by running the command: `su -`

Note: Root level access is disabled by default. To enable root level access a debug capable authentication file with root access support has to be installed and activated on the phone (this procedure is out of scope of this document).

3. For 96x1 H323 phones with P/N 700511225 and 700511227, run the following commands:

```
rtl1836nb_cli
CLI> show_port_status
CLI> show_port_priority_pvid
CLI> show_vlan_table
CLI> show_mac_table
```

To clear the table use:

```
CLI> clear_mac_table
```

(Where: PC port is #1, LAN port is #2 and CPU port is #4)

For other 96x1 phones run the following commands:

```
eth arl table show
```

To clear the table use:

```
eth arl table clr
```

(Where: PC port is #0, LAN port is #1 and CPU port is #8)

5 Text Logs

Extracting steps:

- Serial log
- Avaya Phone log
- Sys Log
- CM log
- Broadcom's log (KNLLOG)

Press **Alt + Left Arrow** to return back to previous view

5.1 Serial Log

Note: Serial Log is already included in Phone Report as Avaya Phone log. It should be provided independently in case the relevant scenario is not included in the phone report.

1. Open Serial shell.

2. Run the relevant scenario and copy all print messages into a file.

Press **Alt + Left Arrow** to return back to previous view 8

5.2 Avaya Phone log

This is the native textual log of the phone. It includes the CLI messages with timestamps and the owner thread.

Note: When Logging mode is OFF, only logs from kernel level will be shown in this log file.

There are two locations for avaya logs:

1. Live log - /tmp/logs/avaya_phone.log
2. Archive - /var/log/avaya_phone.log.[num].gz

Press **Alt + Left Arrow** to return back to previous view

5.3 Sys Log

System logs are written to a volatile memory and containing information mainly regarding performance.

H323 SysLog is already included in Phone Report. It should be provided independently in case the relevant scenario is missing in the phone report. It could also be sent to an external server.

5.3.1 Local Sys Log

H323 System logs are classified according to 8 levels which can be configured via settings file:

SET LOGLOCAL [severity 1-8]
Where severity levels are (default is 7):
  0 - Logging to the MIB is disabled
  1 - Emergency events
  2 - Alert and Emergency
  3 - Critical, Alert and Emergency
  4 - Error, Critical, Alert and Emergency
  5 - Warning, Error, Critical, Alert and Emergency
  6 - Notice, Warning, Error, Critical, Alert and Emergency
  7 - Informational, Notice, Warning, Error, Critical, Alert and Emergency
  8 - Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency
  The output file “logevt” is located at: /AvayaDir/H323/application

Note: Syslog is not affected by the menu option “Logging Mode”.

For SIP 6.2 and on the system logs are also stored in flash. There are up to 3 files stored in the /AvayaDir/SIP/application/LogFiles/:

1. EndpointLog.txt – current capture of system logs
2. EndpointLog_bak.txt – backup of current capture of system logs
3. EndpointLog_prev.txt – capture of system logs up to last time the phone restarted

Press **Alt + Left Arrow** to return back to previous view

5.3.2 Sys Log (sending to an external server)

To send Syslog to an external server:
1. In the settings file set the parameter: SET LOGSRVR [server IP]
2. In the phone go to CRAFT->LOG and change to the required severity.

The relevant content will be taken from “logevt” and will be sent out to the server.

5.4 CM Log

1. Open a shell window to the CM server
2. Navigate to folder /var/log/ecs
3. Upload all log files (*.log) to the PC

5.5 Setting “Logging Mode” parameter to “On”

1. Press “Mute”, ‘C’, ‘R’, ’A’, ’F’, ’T’, ‘#’
2. Scroll down and select “DEBUG” (See “Why DEBUG option doesn’t appear” in section 11)
3. Change “Log to files” to “On”
4. Press “Save”
5. Press “Exit”

Following the above action phones with P/N 700511225 and 700511227 will not reboot, while other 96x1 phone types will reboot at this point.

Note: Due to a known issue, when upgrading/downgrading 6.2.3 from/to 6.2.4, LOGTOFILE value might be undesirably changed. In this case a manual reconfiguration might be required.

Press **Alt + Left Arrow** to return back to previous view 10

6 Demonstrations

6.1 Picture

In case the symptom is seen on the GUI and the scenario might not be reproduced later, use a still camera to capture it.

6.2 Video

In case the symptom can be seen on the GUI and the scenario is reproducible at the field, use a video camera to record the relevant process from the beginning to the end.

6.3 Audio Recording (SIP sets only)

For any audio distortion or damage, record vocal samples into a wave/mp3 file.
SIP endpoints have an embedded audio recording feature.

Note: in some cases it could be an essential info on top of the RTP media capture.

1. Verify the following items are configured in the 46xxsettings file:

```
SET ENABLE_RECORDING 1              ## 0 = off, 1 = enabled (default = 0)
SET WARNING_FILE filename.wav       ## 8 or 16 bit, 8 kHz sample rate G711 A-law or u-
law mono uncompressed WAV file, 100kB max size.
```

2. Enter the A-Menu on the phone (For touch phones go to “Settings”)
3. Select Network Information ->Audio Parameters and press the “Record” soft key
4. The audio report will be generated in the /var/logs/audio_report file.
5. Upload the output file to the PC or copy it to a USB device.

The output is a zip file that contains numerous log files, a packet capture at the Ethernet interface, and 4 PCM files. The PCM audio files are 16 bit Intel PCM (LSB, MSB) 16 kHz file format. Please provide the complete zip file to support/design.

Note: The phone performance will be slowed during the recording and compression process. Do not expect the phone to change screens, IM, Web browse etc. until the compression is complete.

Note: The phone software contains and uses a default English language WARNING_FILE that states “Your call is being recorded”. Record and download the modified WARNING_FILE to match the regional dialect required to comply with the privacy/recording laws of the region.

Press **Alt + Left Arrow** to return back to previous view 11

7 Configurations & Statuses

For troubleshooting and analysis, some field related information is required:

7.1 Settings file

The settings file, named 46xxsettings.txt, should be taken from the HTTP server. For H323 phones, this file could also be gathered directly from the phone:

Open a shell, go to \tmp folder and upload the file “settings_backup.txt”

Note: For H323 firmware the settings file is included in the Phone Report under the file REPORT.txt.

7.2 SNMP MIB data

The SNMP MIB data contains SNMP walk and SNMP logs. Use the string defined in SNMPSTRING in the settings file to create the query in the MIB browser.

7.3 Network Entities

Field network diagram with IP address of the phone and other VOIP related elements, like CM, CLANs, SM, SM100, Media Gateways, etc.

Press **Alt + Left Arrow** to return back to previous view

7.4 Descriptive details

1. What is the symptom? What is the exact user impact?
2. What is the scenario which reproduces the problem?
3. What is the reproduction frequency? How many times the scenario should run until reproduction?
4. What are the affected phone types?
5. What is the software version of the phone and the CM?
6. What is the network topology? What are the network elements in the relevant env?
7. Is there a PC port connected?
8. Is there a Button Module connected?

Press **Alt + Left Arrow** to return back to previous view

8 Obtaining files from the Phone

8.1 Uploading a file to the PC or remote server

8.1.1 Using TFTP:

1. Run a TFTP Server on the PC
2. Use the following command from shell:

```
tftp -p –l [file name] [PC IP]
```

8.1.2 Using FTP:

1. Run an FTP Server on the PC
2. Use the following command from shell:

```
ftpput -u [username] -p [password] [server IP] [destination file]
[local file]
```

8.1.3 Using SCP:

1. Run an SSH Server on the PC
2. Use the following command from shell:

```
scp [local file name] [username]@[remote_server_name]:/[remote_path]
```

8.2 Copying report files to USB (H323 sets only)

On 9611 and 9641 phones, core dump files and phone report can be copied to a USB device.

1. Open shell
2. Connect a storage device to the USB socket.
3. The phone should recognize the USB device and make it accessible under /mnt/h323_usb

Note: In case the phone displays an error “Not enough power…”, unplug any other devices (i.e. BMs) or increase the power by moving the switch on the back panel to “H” state (9608 and 9611 sets only).

4. To see all mounted paths type “mount”.
5. Copy all desired files to the above USB mounted directory.
6. Before disconnecting the USB device, type: `umount /mnt/h323_usb`

9 Opening a Shell

Opening shell connection to the phone can be made in one of the following methods:

- SSH
- Telnet
- Serial

Press **Alt + Left Arrow** to return back to previous view

9.1 Open an SSH connection

1. Ensure SSH_ALLOWED parameter is set to “1” in the settings file.

2. Open an SSH client software, like PUTTY, SecureCRT or any other terminal program.

3. Select SSH2 at the terminal application, and open a connection to the phone’s IP address using port 22.

4. On a first time connection, the SSH client will display the phone’s fingerprint in order for you validate the phone you’re connecting to is actually the one you want to connect to. You can validate this by comparing the displayed fingerprint to the actual phone’s fingerprint. To see the phone’s fingerprint:

- Press “Mute”, ‘C’, ‘R’, ’A’, ’F’, ’T’, ‘#’
- Scroll down and select “DEBUG” (See “Why DEBUG option doesn’t appear” in section 11)
- Select “SSH Fingerprint”

Note: Phones with P/N 700511225 and 700511227 running H323 firmware version 6.6.2 will not display a fingerprint.

5. Login as “craft” user. The terminal will then display a product ID and a challenge code.

6. Use the following Avaya challenge-response tool to get the response ID:
http://ssdp.dr.avaya.com/ASG_WebMobile/index.jsp?lang=en&country=US

Note: Since version 6.2.1, SSH phone reports contain full information.

Note: SSH does not require any special debugging mode state.

Note: For privileged user access, a debug capable authentication file has to be installed and activated on the phone. This procedure is out of scope of this document.

Press **Alt + Left Arrow** to return back to previous view

9.2 Open a Telnet connection

Starting from version H323/6.6.2 and SIP/7.0.1, by default the phone doesn’t support Telnet connection. To enable Telnet connection a debug capable authentication file with Telnet support has to be installed and activated on the phone (this procedure is out of scope of this document). Once the debug authentication file is activated, you can open a Telnet connection to the phone following these steps:

1. Open PUTTY, SecureCRT, or any other terminal program
2. Select “telnet” and connect to the phone’s IP address via port 23

Press **Alt + Left Arrow** to return back to previous view

9.3 Serial Connection (CLI):

Starting from version H323/6.6.2 and SIP/7.0.1, by default the phone doesn’t support serial connection. To enable serial connection a debug capable authentication file with serial connection support has to be installed and activated on the phone (this procedure is out of scope of this document). Once the debug authentication file is activated, you can set the serial connection to the phone following these steps:

9.1.1 Setting “Serial port” parameter to “CLI”

1. Press “Mute”, ‘C’, ‘R’, ’A’, ’F’, ’T’, ‘#’
2. Scroll down and select “DEBUG” (See “Why DEBUG option doesn’t appear” in section 11)
3. Change “Serial Port” to “CLI”

Note: Both CLI and the Button Module use the same serial port hardware. This means that by changing from “Adjunct” to “CLI”, current attached button module would not function and also any future connected button module won’t function as long as the “CLI” is the chosen option. So in order to enable button module devices functionality please remember to change it back to “Adjunct” as soon as debugging is completed.

6. Press “Save”
7. Press “Exit”

Following the above action phones with P/N 700511225 and 700511227 will not reboot, while other 96x1 phone types will reboot at this point.

Press **Alt + Left Arrow** to return back to previous view 13

9.1.2 Open a Serial Connection:

1. For serial port connection it is required to obtain the Avaya Service Adapter, P/N 700504366. This adaptor includes a serial cable that connects the phone's Button Module port to a PC's USB port, which allows a serial console access to the phone.

Avaya Service Adapter

Installation and configuration instructions of the Service Adapter, as well as driver information can be found in the following document:

https://downloads.avaya.com/css/P8/documents/100172896

2. Open PUTTY, SecureCRT, ProComm or any other terminal program
3. Connect the serial cable, so one end is connected to the MOD port on the phone, and the other end is connected to the Service Adapter jack with the phone label. Connect a USB cable between the Service Adapter and your PC.
4. Set the following values at the terminal program:
   115200 bps, 8 data bits, no parity, 1 stop bit, no flow control.

Press **Alt + Left Arrow** to return back to previous view

10 Collecting Broadcom’s logs (KNLLOG)

Note: This procedure requires privileged user shell access.

1. Type the following commands via the phone shell:

```
echo 100000 > /proc/sys/knllog/entries
echo 1 > /proc/sys/knllog/deltatime
echo 14 > /proc/sys/knllog/irq_sched_enable
echo 0 > /proc/sys/knllog/enable
```

Note: Broadcom’s kernel logs include various information details, which might not necessarily required in all cases and might also affect the phone’s performance. Please use this section as an example only and consult R&D for which and how data to collect in each case.

2. Now, for each specific event which you would like to record, type the following commands. These commands will capture 10 seconds of kernel activity.

```
echo 1 > /proc/sys/knllog/clear
echo 1 > /proc/sys/knllog/enable
sleep 10
echo 1 > /proc/sys/knllog/dump
```

3. Upload the output file (/tmp/knllog.txt) to the PC or copy it to a USB device (for instructions see section 8).

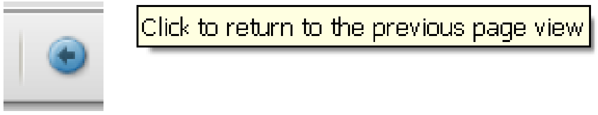
Press **Alt + Left Arrow** to return back to previous view 14

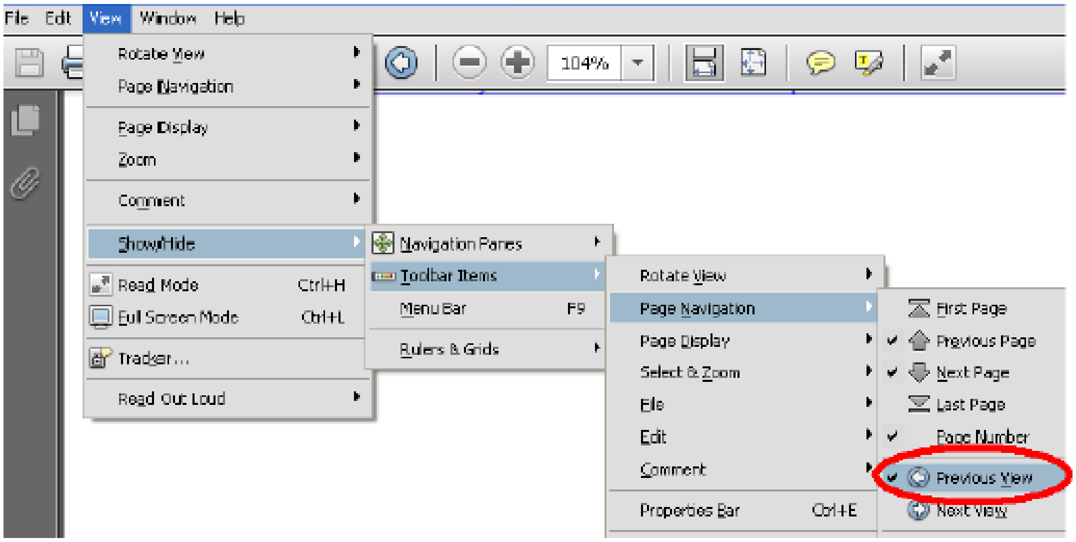
11 Why DEBUG option doesn’t appear?

The DEBUG option is available for use only for non-default passwords (different than “CRAFT”). To set a new password for the craft menu, change PROCPSWD parameter in the settings file. The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However if value of PROCPSWD is less than 4 digits, the value will be changed back to the default value of 27238 (CRAFT).

Acrobat Reader tip:

After clicking a hyperlink, you can return back to the original place through a button.
To add the “previous view” button, select “View” from the menu, then select:
“Show/Hide” → “Toolbar Items” → “Page Navigation” → “Previous View”.
For further information regarding on site debugging, see H323 serviceability presentation at:
https://projects.share.avaya.com/sites/96x1_H323/Alpha/Documents/H32362servicability.pptx


Click to return to the previous page view


File
Edit
View
Window
Help
104%
Rotate View
Page Navigation
Page Display
Zoom
Comment
Show/Hide
Read Mode Ctrl+H
Full Screen Mode Ctrl+L
Tracker...
Read Out Loud
Navigation Panes
Toolbar Items
Menu Bar F9
Rulers & Grids
Rotate View
Page Navigation
Page Display
Select & Zoom
File
Edit
Comment
Properties Bar Ctrl+E
First Page
Previous Page
Next Page
Last Page
Page Number
Previous View
Next View