

## **Comdasy** FAQ: Network Tracing

Comdasy AG  
Rüdesheimer Str. 7  
D-80686 München  
Tel.: +49.89.5484333-0  
Fax: +49.89.5484333-29

[support@comdasy.com](mailto:support@comdasy.com)

<http://www.comdasy.com>

## **Disclaimer**

We have taken all possible care to ensure that this manual contains correct, accurate information. However, the manufacturer cannot assume liability for any possible errors. In addition, the manufacturer cannot guarantee that the hardware will meet the purpose you require.

Comdasys reserves the right to make changes according to technical progress at any time. Brand names may be registered trademarks and must be treated as such.

© Copyright 2005-2008  
Comdasys AG  
80686 München, Germany

All rights reserved. No part of this manual may be reproduced, processed or distributed in any form (print, photocopy, microfilm or any other process) or processed by an electronic system without prior written permission from the manufacturer.

# Content

1. Synopsis.....	4
2. NTP.....	4
3. Via the Web Interface (Version 6719.x).....	4
4. Tracing in the CLI.....	4
4.1. Steps and arguments.....	4
4.2. Example.....	5
5. tcpdump and Etherreal.....	5
6. Questions and Answers.....	5
6.1. Discrepancies in older versions.....	5
6.2. Convergence with or without Integrated Gateway.....	6
6.3. Tracing loadtests with Convergences.....	6
6.4. Tracing without Restart.....	7

## 1. Synopsis

If an error occurs in your network and you need support from Comdasys, it is recommended to provide the support team with in-depth information in the form of traces. This enables the support team to quickly analyze the problem sources.

All our Convergence and Mobile Convergence products have built-in means for tracing which are accessible via their respective web interfaces or via the command line interface (CLI).

For efficient and quick support, traces should fulfill certain standards. This document describes how to capture traces which meet these standards.

## 2. NTP and Tracing

**It is strongly recommended to have clock synchronized with NTP on all devices involved!**

If this is not the case, comparing time differences will not be possible in a consistent and reliable way.

## 3. Via the Web Interface (Version 6719.x)

There are two different menus for tracing in the web interfaces of all our products:

1. **Network Trace:** enables you to select a specific interface of your device (WAN, LAN etc.) for tracing Ethernet traffic. You can modify this and also collect syslogs via the CLI.
2. **Support Trace:** this menu has been designed to help customers whenever they are in need of support. The Support Trace collects various information about your running system, which can be very helpful for remote error analysis. This comprises: Ethernet trace, syslog in separate file, system version and various diagnostic data



If the SIP Proxy of your (Mobile) Convergence is in use, current phone calls will be interrupted when the *Support Trace* is started! Therefore, it might be necessary to re-register your phones!

Both of these menus are explained in thorough detail in our Administrator Manual.

## 4. Tracing in the CLI

The tracing tool that is used by your (Mobile) Convergence in the background is [tcpdump](#). The command line interface gives you the possibility to further modify the tracing parameters used by this built-in tracing tool. It is also possible to visualize the traces in the CLI by using [tcpdump](#), but you may also save them and process them further with tools like [Etherreal](#) or [Wireshark](#).

The following provides a brief introduction of the usage of [tcpdump](#) via the CLI.

### 4.1. Steps and arguments

Open a shell and log onto your (Mobile) Convergence (via PuTTY for Windows) and execute the command `tcpdump`. How tracing is performed can be modified with the following arguments:

- `-i`  
This option is used to indicate the interface that the packets are being captured from.



The parameter “any” is the default interface for tracing in version 6719.x, but has to be set manually in 4675.x.

- `-s 0`  
Usually only the first 64 bytes of a packet will be traced. This reduces especially the size of long running traces. Please note that traces especially on the LAN interface can get very large rather quickly if no filters are specified. The `-s0` parameter will remove the 64 Byte limitation. The entire packet including the payload will be visible in the trace file. It is also possible to specify a different (limited) length by using: `-s <number of bits>`



This is as well a default parameter in version 6719.x, but has to be set manually in 4675.x.

- `port <port number>`  
This will introduce a filter into the trace only for the packets with source or destination.
- `src host <IP address>`  
This will restrict the tracing to all packets coming from the specified host.
- `dst host <IP address>`  
This will restrict the tracing to all packets going to the specified host.
- `proto tcp`  
You could also use protocols ip, icmp, udp here. This will trace only the specified packets.

#### 4.2. Example

```
tcpdump -n -i any -s 0 -A port 5060 and host 10.42.1.20
```

`-n` = disable DNS

`-X` = makes the packet content visible in the console in ASCII format.

`-i any` = all interfaces (mandatory for LAN/WAN scenarios)

`port 5060` = SIP only

`host` = only from/to the IP of the Convergence

## 5. tcpdump and Ethereal

In order to capture the raw data for later analysis with Ethereal use: `-w <filename>`

**Example:**

```
tcpdump -n -i any -s 0 -w /tmp/trace.cap
```

Traces should generally be saved to the temporary files. This makes sure that they will not take up memory for ever. The file name "trace.cap" above is just an example, you are free to choose a different file name.

The file can then be copied to a separate machine for further processing (use SCP or WINSCP for transfer).

## 6. Questions and Answers

Some short questions have accumulated over time which will be answered in the following.

### 6.1. Discrepancies in older versions

Naturally many bugs have been fixed since version 4675.x. A common problem regarding tcpdump in that version was that it was running with the wrong priority. This resulted in messages such as "TCP : previous segment ACK lost". Please consult our [sales department](#) for information about updates/upgrades.

### 6.2. Convergence with or without Integrated Gateway

This is how you can collect comprehensive traces on a ConvergenceGW:

1. Go to the VOICE tab and enable debugging in the *Diagnostics* menu.
2. Open the *Logging* menu in the DIAGNOSTIGS tab and set the *Syslog Server* to the built-in syslog server 127.0.0.1 and set the *Log Level* to *Debug*. This will not send syslogs anywhere, but just allow it to be visible in tcpdump traces.  
  
If you already have some IP address here of your external syslog server, than changing it to 127.0.0.1 isn't necessary.
3. Then open the GATEWAY tab. Go to *System* → *Syslog* and activate *Enable diagnostic traces*.
4. Go back to the DIAGNOSTICS tab of the Convergence part and set the *Interface* in the *Network Trace* menu to ANY.
5. In the last step click *Start* to start the trace and *Stop* when enough information has been gathered.

To perform this tracing on a Convergence without integrated gateway, simply leave out Step 3.

#### Advantages of this method:

- The result are SIP Proxy logs including network traffic in one .cap file
- Traffic on all interfaces (including loopback interface) is captured
- Time relations between packets and syslogs can be compared conveniently (please make sure that NTP-based clock synchronization takes place)

### 6.3. Tracing load tests with Convergences

If you would like to perform tracing during load tests, this is how it is done without TLS:

1. Enable debugging in the Diagnostics menu of the VOICE tab.
2. Set a valid external syslog server in the DIAGNOSTICS tab and set the Log Level to *Debug*. Please disable the *Local File*.
3. Run Wireshark in a ring buffer on a relevant switch mirror port and set the following configuration: use multiple files: yes, next file: each 15MB, Ring buffer with 30 files  
15MB is the maximal pcap size for optimal use.

With TLS:

1. Proceed as described above. However, it will not be possible to decrypt all pcaps except the first one.
2. If an error happens fast enough it could be possible to use just one big pcap and limit capture to traffic on SIP/TLS ports only with the capture filter: `port 5060 or port 5061`  
100MB is the the maximum size for pcap which is still usable (in extreme cases).

### 6.4. Tracing without Restart

Errors coming from the SIP Proxy can be solved by restarting it. Do the following to perform tracing without restarting the SIP Proxy:



This is based on the system with the following settings:

- Debugging is enabled under VOICE → *Diagnostics*
  - The *Syslog Level* in the DIAGNOSTICS tab is set to *Warning*
1. Change the *Syslog Level* to *Debug* without clicking *\*Apply Configuration\**
  2. Go to the *Home* page and “Reapply Configuration” (far-right button) on the the *Syslog Daemon* (right-hand side under *Diagnostics*) then restart the Syslog Daemon (middle button):

Availability		[Green]	
Diagnostics		[Green]	
	Service	Action	
[Green]	Cron daemon	[Off]	[Restart]
[Green]	Kernel log daemon	[Off]	[Restart]
[Grey]	SNMP daemon		[Refresh]
[Green]	Syslog daemon	[Off]	[Restart] [Refresh]
Routing		[Green]	
VoIP		[Green]	

3. After you have collected sufficient traces, revert your changes in the same way.