



The Power of We™

## TECHNICAL WHITE PAPER

# Avaya Communication manager File Synchronization overview and Troubleshooting

---

### Abstract

This paper discusses some of the challenges associated with failure of File (translation) synchronization between Avaya Communication Manager Core/Main servers to Survivable servers

This document will help in resolving and quickly isolating the cause for some of the most commonly known issue with respect to file sync failures

### Topics

- 1 Terminologies
- 2 Introduction
- 3 Frequency of File Synchronization
- 4 File Synchronization Process
- 5 Troubleshooting
  - 5.1 How to check Filesync status
  - 5.2 Troubleshooting file sync on Duplex server
  - 5.3 Troubleshooting filesync on LSP/ESS servers
- 6 Conclusion



The Power of We™

## 1. Terminologies

CM - Avaya Communication Manager

ESS - Enterprise Survivable Server

LSP - Local Survivable Processor

Main - The currently active server which is controlling the entire network. It is the source of files that are synchronized to the other, target servers.

SAT - System Administration Terminal interface to the telephony application on an Avaya

xln1 - translation file saved on the disk when we run “save translations” command

## 2. Introduction

When multiple servers (i.e. processors) are present in a network, the active server shares configuration information (translations) with all the other servers (standby server and LSP/ESS servers) so that in the event of failure, a surviving processor can take over and have the latest information.

File synchronization actually transfers a number of files between the servers. However, the largest of these is the Avaya Communication Manager translation file

Sharing occurs in a process known as file synchronization (filesync) and can happen once per day or whenever the translation file is changed. The system must be operated in a manner, and the network connectivity designed, to accommodate this activity.

### 3. Frequency of File Synchronization

File synchronization can be initiated any time by the SAT command

```
save translations [lsp|ess|all]
```

is performed. This command can be executed by a SAT user and can also be executed during the daily maintenance if the '*system-parameters maintenance*' form has been administered to do so.

File synchronization also occurs to a specific LSP/ESS when the LSP/ESS registers with a server, if the translations file on the LSP/ESS differs from the one on the server.

Note:- The SAT command *save translations [lsp|ess]* should not be executed more frequently than the transmission bandwidth available to accomplish the file synchronization.

#### Translation File Size:-

The translation file is saved on disk in the file

/etc/opt/defty/xln1.

The size of this file can be obtained from the Linux shell command `ls -lt` as follows:

```
ls -lt /etc/opt/defty/xln1
```

The size of this file varies widely depending on the number of stations, the number of trunks, and the combination of features that are used.

### 4. File Synchronization Process

When a save translations SAT command is issued, the following actions take place:

1. The SAT command attempts to save the translations in the local xln1 disk file.
  1. This write could fail if the file synchronization code has xln1 *locked*. In this case the message *save translation has a command conflict* is displayed to the SAT user. (Cf. step 4.)

2. The SAT command signals the file synchronization code to perform an update.
3. The SAT save translations command causes a 300 second timer to start.
  1. If the file synchronization code is currently processing an update as a result of a prior save translations and if it continues to be busy for 300 seconds, the SAT command will time out and display the following message to the user: *Standby comm not up*. In this case, the file synchronization request is queued and will be honored after the file synchronization code has processed all prior requests
4. The file synchronization code locks the translation file, xln1, and updates the standby server (if there is one). When the standby is updated, the lock on xln1 is released and the SAT is informed that the standby has been updated.
5. If there are LSP/ESS servers to be updated, a compressed copy of xln1 is made and locked. This compressed copy is then synch'd to the LSP/ESS servers. The file synchronization code updates LSP/ESS servers one at a time. This is done as follows:
  1. The next LSP/ESS is selected for update
  2. A 300 second timer is started
  3. A determination is made as to whether a file transfer must take place. i.e. is the LSP/ESS already up to date.
  4. If data is to be transferred, transmission begins.
6. When the transmission completes, return to step (5.1) if there are additional LSP/ESS servers to update. If the timer of step (5.2) expires before the transfer in step (5.3) completes, the transfer to the current LSPs is terminated and processing continues at step (5.1) for the next LSP. There is no re-try.

Note carefully from the above, that each LSP/ESS is allowed 5 minutes (300 seconds) to complete an update. If the update cannot be completed in this time regardless of cause (slow network, busy processor, etc.) that LSP is not updated.

If translations are saved more frequently than the file synchronization can transfer the files (step 5 above), the synchronization requests are queued. Each time file synchronization runs, the latest available copy of the translation file is synchronized. If multiple jobs are queued and no additional save translation is performed, the queued jobs will not actually transfer a file. The file synchronization code determines that the file on the far end is up to date and no file is transferred.

## 5. Troubleshooting

File synchronization can be affected by the following:

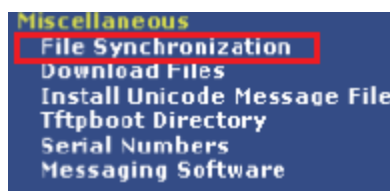
- The size of the translation file
- The load on the call server (processor occupancy)
- The frequency of translation saves
- The network bandwidth and connectivity available from the active server to each of the other servers
- The number of ESS/LSPs.

Below instructions is some of the most commonly used Procedure to troubleshoot file sync issues

### 5.1 How to check File Sync status/Summary:

#### File Synchronization status via Web Menu Access :-

File synchronization status can be checked via CM maintenance webpage, under the miscellaneous group *as* illustrated in figure 1



**Figure 1.** Menu Link for File Synchronization



The Power of We™

## File Synchronization status via Linux shell command:-

**filesync -H <type>**

History of last 25 translation syncs to servers of the specified type. TYPE: 'all', 'dup', 'ess', or 'lsp'.

**filesync -q** query status of most recent Sync

## Filesync Alarms:-

When the file sync fails , main server will generate FSY 1 Minor alarm

## SERVER ALARMS

=====

ID	Source	EvtID	Lvl	Ack	Date	Description
1	FSY	1	MIN	Y	Tue Apr 8 01:47:31 2008	file sync failed for XXX (where XXX points to endpoint)
0	FSY	1	MIN	Y	Tue Apr 8 01:44:19 2008	file sync failed for XXX (where XXX points to endpoint)

## 5.2 Troubleshooting file sync on Duplex server

- Verify that filesyncd is running on the server **statapp** from the bash, see filesyncd process is UP 8/8

```
-
init@B1R2-Server1> statapp
Watchdog          19/19 UP
TraceLogger       3/ 3 UP
ENV               1/ 1 UP
LicenseServer     3/ 3 UP
SME               9/ 9 UP
MasterAgent       1/ 1 UP
MIB2Agent         1/ 1 UP
```

©2014 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.



The Power of We™

MVSubAgent	1/ 1 UP
LoadAgent	1/ 1 UP
FPAgent	1/ 1 UP
INADSAAlarmAgen	1/ 1 UP
GMM	4/ 4 UP
SNMPManager	1/ 1 UP
arbiter	2/ 2 UP
<b>filesyncd</b>	<b>8/ 8 UP</b>
dupmgr	1/ 1 UP
MCD	1/ 1 UP
CommunicaMgr	85/85 UP

If the process is not running , you can always start is using command “**start –s filesyncd**”

- Verify you can ping the standby server

**ping** the standby server, both over the dup link and the eth4 interface

**pingall –d** should pass (this command will work only on CM 5.x and below, you need to ping the standby duplication link IP address and server IP’s on CM 6.x)

if you’re not able to ping, filesync won’t work

- Verify the dup link is up and the standby is refreshed

execute the **server** command from the bash and ensure:

*Standby Refreshed: Yes*

*Standby Shadowing: On*

*Duplication Link: Up*

- Verify the Ethernet interfaces on the servers are setup appropriately

On CM 5.x and below:-

run **setnic –q eth2** on CM linux shell and ensure the link is running at 100/Full for Hardware Duplicated servers For software duplicated server eth0 should be locked to AUTO. It will negotiate itself to 1Gbps

or you can verify the speed duplex settings on **Configure server – Configure interface Link** on CM web page , as illustrated in figure 2 .

**Configure Individual IP services**

- Review Notices
- Server Role
- Set Identities
- Configure Interfaces**
- Configure UPS
- Set DNS/DHCP
- Set Static Routes
- Configure Time Server
- Set Modem Interface

## Configure Server

\* = required fields

### Ethernet 0: Control Network A, Processor Ethernet (PE), Corporate LAN Interface

IP address server1 (S8730CM521Serv1)  \*

IP address server2 (S8730CM521Serv2)  \*

Alias IP address, active server (S8730CM521)  \*

Gateway  \*

Subnet mask  \*

Speed (Current speed : AUTO SENSE) 100 Megabit full duplex \*

☐ Enable VLAN 802.1q priority tagging

### Ethernet 1: Laptop Interface

IP address server1 192.11.13.6

Subnet mask 255.255.255.252

### Ethernet 2: Server Duplication Interface

IP address server1 (S8730CM521Serv1) 192.11.13.13 \*

IP address server2 (S8730CM521Serv2) 192.11.13.14 \*

Subnet mask 255.255.255.252 \*

Speed (Current speed : AUTO SENSE) 100 Megabit full duplex \*

**Processor Ethernet (PE) Parameters**

Figure 2: Configuring speed duplex settings on CM 5.x and below

On Cm 6.x, the Ethernet interface Speed should be set to Auto-Neg so that it will negotiate 1G full duplex speed.

By default the server eth3 interface will be used as duplication link (this can be changed if needed)

You can check the speed duplex settings on “ethernet configuration” under server management in the System platform web interface, as illustrated in figure 3



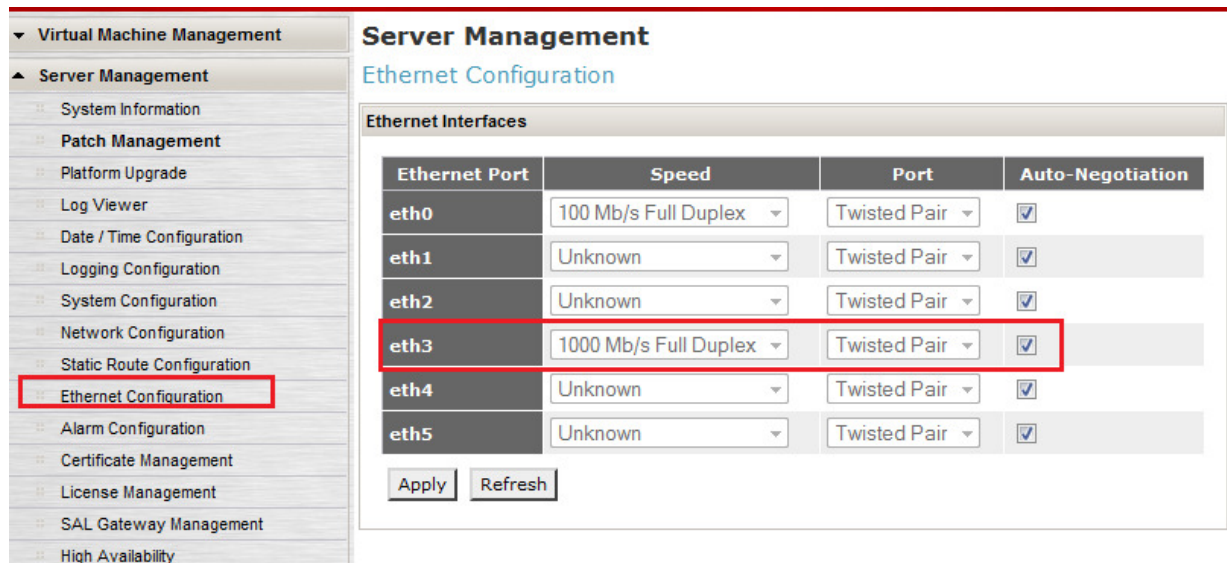


Figure 3: Configuring speed duplex settings on CM 6.x

- Make sure that active and standby server has same patches installed by running “swversion” command via Linux shell.

```
admin@Main_server1> swversion

Operating system:  Linux 2.6.18-128.AV07PAE i686 athlon
Built:  Aug 19 04:58 2009
Contains:  02.1.016.4
CM Reports as:  R015x.02.1.016.4
CM Release String:  S8720-015-02.1.016.4

UPDATES:

Update ID          Status      Type      Update description
-----
02.1.016.4-18576   activated   cold      patch 18576 for 02.1.016.4
```

## 5.3 Troubleshooting filesync issues to LSP and ESS

- Verify filesyncd process is up and running in all servers using Linux bash command **statapp**.

```
init@B1R2-Server1> statapp
Watchdog          19/19 UP
TraceLogger       3/ 3 UP
ENV               1/ 1 UP
LicenseServer     3/ 3 UP
SME               9/ 9 UP
MasterAgent       1/ 1 UP
MIB2Agent         1/ 1 UP
MVSubAgent        1/ 1 UP
LoadAgent         1/ 1 UP
FPAgent           1/ 1 UP
INADSSAlarmAgen  1/ 1 UP
GMM               4/ 4 UP
SNMPManager       1/ 1 UP
arbiter           2/ 2 UP
filesyncd        8/ 8 UP
dupmgr            1/ 1 UP
MCD               1/ 1 UP
CommunicaMgr      85/85 UP
```

If the process is not running , you can always start it using command “**start -s filesyncd**”

- Make sure LSP/ESS has **equal or later software version and patch** than main server.
- CM 5.X and or above in LSP/ESS will not sync with CM 1.X in Main
- Verify that the ESS/LSP is currently registered in SAT using command **list survivable-processor** and **status ess cluster**
- Verify the time of the last successful filesync using the SAT command **display lsp, list survivable-processor** and **status ess cluster**
- Ensure that you can **ping** the target ESS/LSP from the Linux shell and verify that the correct interface (customer LAN) is being used to reach it using **traceroute**.

- Run a **tracert** from the S8xxx to the LSP and from the LSP to the S8xxx; capture the results in a file and ensure the packets aren't getting delayed on specific hops
- **Verifying that the network is permitting filesync traffic**

Verify that connections on this port traverses the entire enterprise network from the main server to the destination (ESS or LSP) server. To do this, access the Linux bash prompt on the main server, and use the telnet tool with its optional port specification:

```
telnet <destination_server_IP> <portnumber>
```

where **<destination\_server\_IP>** is the user's LAN port IP address of the ESS or LSP, and **<portnumber>** is the port number tested above.

***Note:** use port number 21874 if the CM version is 3.x and above  
use port number 21873 if the CM version is below 3.x*

Telnet is very close to a raw socket connection with little overhead, so simply establishing a telnet connection on the appropriate port verifies that the port in question is open all the way through the network. To any network devices/routers/firewalls in the path, this connection attempt looks identical to a filesync connection for pushing translations. Any policy configured that affects the filesync also affects this connection attempt.

### **Result 1 - Success**

A successful connection looks like this:

```
inads@S8700B-N1> telnet 168.109.61.11 21874
Trying 168.109.61.11...
Connected to 168.109.61.11.
Escape character is '^]'.

```

To close the connection, press 'Control+]' and type close at the telnet> prompt, like this:

```
^]
telnet> clo
Connection closed.

```

NOTE: It is not possible to do anything through this telnet connection, it is simply verifying whether the port number is open from end to end.

This outcome suggests that filesync is working, at least from a TCP reachability standpoint.

### ***Result 2 - Unreachable on filesync port***

If the connection is never completed and eventually times out from the main server, it is a strong indication that the packets on that port are being silently dropped somewhere in the network. This includes the destination server if it is not verified whether the port is open in the IPtables firewall. IPtables also perform a silent drop or ignore of packets to closed ports.

If the connection attempt stops quickly with a message that the connection failed or is reset, that typically indicates a firewall is configured to reset connections that are not permitted.

### ***Result 3 - Connection completes and is immediately closed***

The last possible outcome of the connection is that the socket is successfully opened, but is immediately closed by the destination server, with output such as this:

```
inads@S8700A-N1> telnet 168.109.61.11 21874
Trying 168.109.61.11...
Connected to 168.109.61.11.
Escape character is '^]'.
Connection closed by foreign host.
```

In this case, the connection is immediately closed and the user does not require to type 'Control+] to stop it. This typically indicates that the port is open all the way from the main server to the destination server, but the destination server is not expecting a filesync connection from the source IP address that is being used. This indicates a misconfiguration on the ESS/LSP, such as a virtual address being defined on the ESS/LSP's. Configure Identities page instead of an actual IP address of a main server.

- **Ping** the LSP/ESS with a packet size of 1500bytes to see if there are Network related problems.

Issue a **ping -s 1472** (LSP/ESS IP Address) ---> this is 1500 with overhead



The Power of We™

If it fails, most likely this might be the cause. One way to confirm if this is the case is to transfer the Translation files (xln files) from the Main Site to the ESS/LSP using FTP. If that works, then the Network is not the cause of the problem.

- Verify that the IP address customer LAN interface of both S8xx0 servers are listed in the file **/etc/ecs.conf** next to the entries **SRAYPA1** and **SRAYPA2** in ESS/LSP
- Check **date and timezone** in LSP/ESS, they should be the same following the timezone rules
- Make sure that all customer **LAN ethernet interfaces** of Main, LSP and ESS are locked to **100Full** in case of CM 5.x and is set to **Auto-neg** and the current speed and duplex shows **1G Full**.
- Try **stopping and starting the filesyncd** process on LSP/ESS by using command

```
stop -s filesyncd
start -s filesyncd
```

- Check whether PKI is expired or not using bash command. The output of the below command should not be a date in past.

```
root@B1R2-Server1> cd /etc/opt/ecs/certs/server
root@B1R2-Server1> openssl x509 -in server.crt -noout -
enddate
notAfter=Jun  7 15:07:47 2020 GMT
root@B1R2-Server1>
```

**Note:** In **CM 6.x**, certificate is located in **/etc/opt/ecs/certs/cm/ID** Directory

- Verify that this is a not a Firewall issue. One way to confirm this without being concerned about what Release of CM the LSP/ESS or the Main Server is running on (certain CM Releases uses different Ports for Filesync) is to shut down the Firewall on both ends. Issue a "**service iptables stop**" on both ends (Main and ESS/LSP). This is a bash command and has to be done with root privileges.

**Note:** - Stopping IPTables will disable internal Linux firewall, Please advise Customer and Business partner before stopping the IPTables..

- Once the above command is done, go into SAT and then issue a "save translations ess/lsp" command. If it still doesn't work, then make sure that the Firewalls are turned back on by issuing a "service iptables start" command. After stopping iptables if filesync works then analyze the settings of the firewall and general port status. These ports should be open in customer network firewalls also.
- **CM 1.X uses ports 514/TCP and 512-1023/TCP port 1022** may be commonly blocked due to the Sasser worm's utilization of it, thus customers must either allow this port specifically between the S8700 and the LSP or they have to upgrade
- **CM 2.X uses port 21873/TCP**
- **CM 3.X and above uses port 21874/TCP**
- perform `netstat -an | grep <filesync_port>` > /tmp/netstat1  
tcp 0 0 0.0.0.0:21874 0.0.0.0:\* LISTEN

perform `netstat -nr` > /tmp/netstat2

verify the results are appropriate for the load of software (i.e. the appropriate ports are open)

- Make sure scheduled backup and system maintenance is not configured at the same time. Also save trans should not be enabled in scheduled backup from a standby server. Display system-parameters maintenance will show you the time for scheduled maintenance and scheduled backup from web interface will show you the time for scheduled backups

## 6 Conclusion :-

The above details will help you isolate File synchronization issue from system generated to network side issue. You can follow the above Steps to investigate & resolve the commonly known issues.

Once you have gone through the above steps correctly and done the initial troubleshooting if there the issue is still observed, you can open a Service Request via [www.support.avaya.com](http://www.support.avaya.com) our experts will help you to root cause & fix your issue.