Documentation

HiPath 4000 V5
IP Solutions - Disaster Recovery

Service Documentation

A31003-H3150-S104-2-7620

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

SIEMENS

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

Reference No.: A31003-H3150-S104-2-7620

Service Manual HiPath 4000 V5 - IP Solutions - Disaster Recovery - Contents

1 Feature Description

The feature „Disaster Recovery“ offers enhanced survivability functionality. It is possible to install a second HiPath 4000 system which can be activated by the administrator in the case of a disaster with consequences which last long, e.g. fire, water damage or a hurricane. The disaster recovery system takes over the functions of the main system.

1.1 Scenario

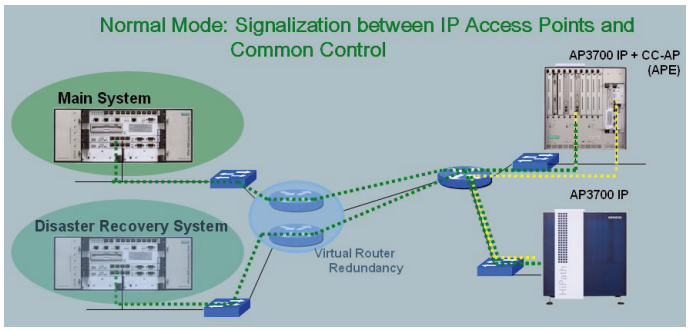

Figure 1 *Normal mode signaling and synchronization of main system and disaster recovery system*

The main system is destroyed. The connected IP access points detect that the signaling to the main common control (CC-A / CC-B) is not possible and will fallback automatically to the configured CC-AP (normal AP-Emergency Mode).

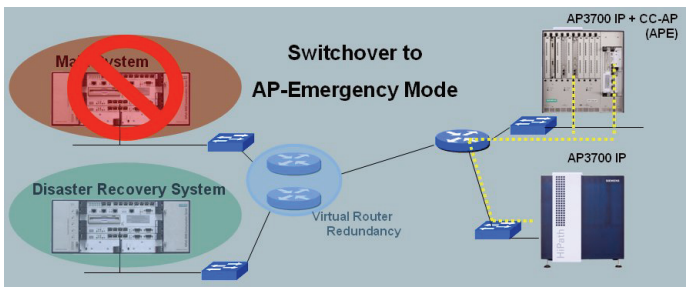

Figure 2 *AP Emergency mode*

Activate disaster recovery (standby) system while AP emergency mode is still active.

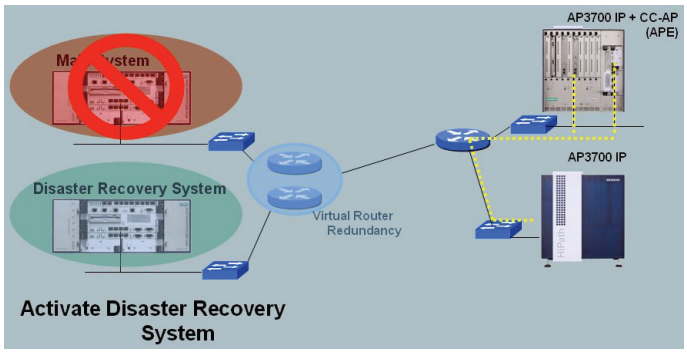

Figure 3 Activate disaster recovery (standby) system.

Main system is disconnected from the network and now the switch over must be invoked on the disaster recovery (standby) system. Now the IPDA-LAN-Ports on the processor boards (CC-A/CC-B) of the disaster recovery system are automatically activated. The HiPath 4000 Assistant IP address of the disaster recovery system has been changed automatically, so that all IP addresses of CC-A/CC-B/ADP are the same as the main system before.

If the common control of the disaster recovery system is active and reachable for all AP3x00 IP in the customer network then the AP3x00 IP will switch back from CC-AP to the disaster recovery system.

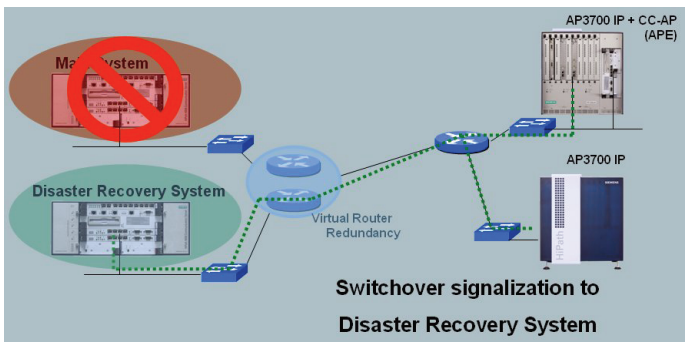

Figure 4 Signaling after switch over to disaster recovery system

1.2 Prerequisites

- Two HiPath 4000 systems (one as the main system and the second as disaster recovery (standby) system).
- IPDA LAN interface for Access Point Emergency in order to connect the access points in the customer LAN to the HiPath 4000 main system (TCP/IP connection).
- The **Disaster Recovery** concept assumes the network of main system, disaster recovery (standby) system and the feature **Access Point Emergency**. For more information on the installtion of the feature **Access**

Point Emergency please refer to the documentation „IP Distributed Architecture (IPDA) and Access Point Emergency (APE)“, Chapter 5, “Configuring the APE Feature (Access Point Emergency)”.

- Only IP access points (AP3x00 IP) are supported.
- Subscribers directly connected to the main system can no longer be used in case of disaster recovery mode.
- Applications redundancy is required (e.g. ProCenter using Atlantic LAN)
- The main and disaster recovery (standby) system has the same hardware and software version, but of course e.g. hardware ID or IP address in C-LAN are different.
- There must be a connectivity on C-LAN between main system and disaster recovery (standby) system.
- The common controls of main system and disaster recovery (standby) system must have the same IP address, so that both common controls will address the same broadcast domain. Because of the fact that the IPDA port is deactivated on the disaster recovery system no IP address conflict occures on IPDA (in AP emergency mode).

1.3 Service Information

- The feature „Disaster Recovery“ has been released with HiPath 4000 V4 R2 and HiPath 4000 Assistant V4 R3.
- „Disaster Recovery“ **does not** replace any type of data backup.
- Subscribers directly connected to LTUs Shelfs of the main system can no longer be used in case of disaster recovery mode. These subscribers need to be moved to other shelfs, that are connected directly to the disaster recovery switch.
- For configuring the feature „Disaster Recovery“ use the HiPath 4000 Assistant application „Disaster Recovery“.

  For more details please refer to Chapter 2, “First Installation”.
- The **synchronization** between main system and disaster recovery (standby) system is done by HiPath 4000 Assistant application **Backup & Restore**.
  - The Unix part is synchronized by data backup. From main system a backup is periodically transferred to an FTP server. The disaster recovery (standby) system periodically checks if new backup is available on FTP server. If so, it downloads the backup from the FTP server and then restores it.
  - In RMX only PDS area (A1H1E) is synchronized.

  - For more details please refer to Chapter 2, “First Installation”.

- Codeword Tool (CWT)

  The codeword tool (CWT) saves one codeword for the master system and another codeword for the disaster recovery system (in a zip file) under the master system entry. These two codewords and the associated SIM cards only work together in conjunction with disaster recovery. If you use a different codeword or SIM card, disaster recovery system administration is impossible following changeover to the "productive switch".

1.4 Restrictions

- For Disaster Recovery a project specific release (PSR) is necessary.
- Disaster Recovery is only released for cPCI hardware.
- The disaster recovery (standby) system will not be registered at the HiPath 4000 Manager.
- The switch over must be done manually (e.g. by a customer administrator). Customer administrators are be able to control the switch over to the disaster recovery system.

synchronization

DR Backup on main system and subsequent DR Restore on disaster recovery (standby) system is called synchronization.

2 First Installation

2.1 Disaster Recovery Flag

After first installation every system is in main mode and the disaster recovery flag (AMO CPCI, parameter **DISREC**) is set to **NO**.

The flag can be set either with the AMO CPCI or the HiPath 4000 Assistant application **Disaster Recovery**.

The staus of the flag can be displayed with `DISP-CPCI:DATTYP=SYS;`. The status of the flag can also be seen in the home page of the HiPath 4000 Assistant application **Disaster Recovery**.

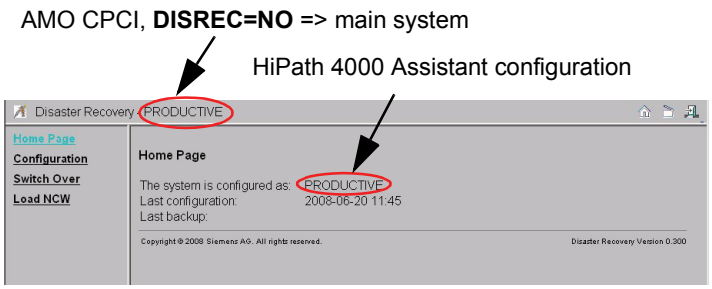

Figure 5 *Disaster recovery flag in HiPath 4000 Assistant application „Disaster Recovery“*

2.2 Main System

2.2.1 Configuration as Main System

1. Turn on **Disaster Recovery** application in HiPath 4000 Assistant

---

NOTE: Configuring system to productive mode in HiPath 4000 Assistant induces starting of some processes (such as CM, COL, PM etc.).

Base Administration > Application Control

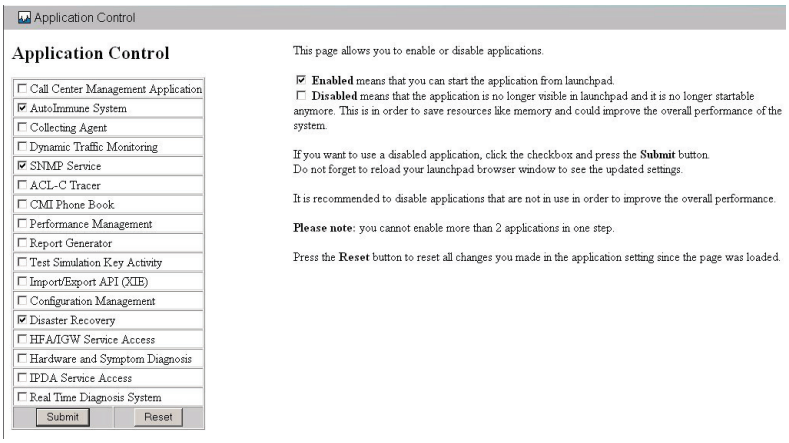

Figure 6 Disaster recovery application

2. Configure the system as main system in HiPath 4000 Assistant

   Software Management > Disaster Recovery > Configuration

   Select the button **Configure as Productive**.

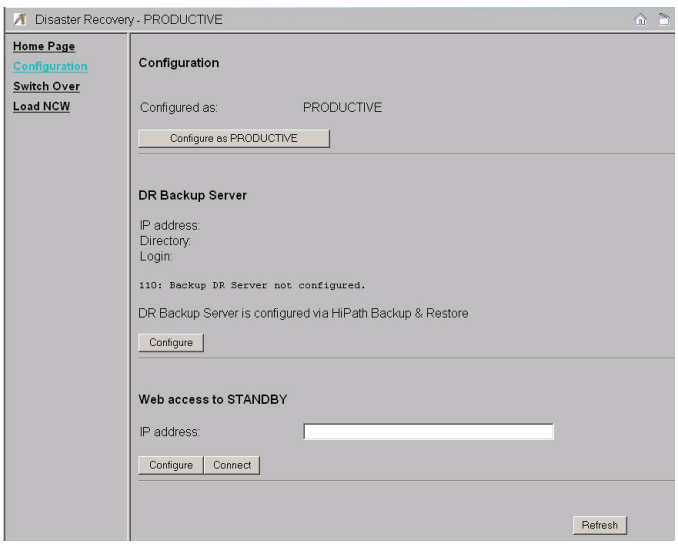

Figure 7 Disaster recovery configuration (main system)

Following actions are automatically done:

- The disaster recovery flag is set to **NO**. You can check the status of the flag in AMO CPCI, **DISREC=NO** and HiPath 4000 Assistant **Disaster Recovery**. With this configuration of the disaster recovery flag the IPDA LAN interface is initialized and a connection to the access points exists.
- Some processes are started (e.g. Performance Management, Configuration Management, etc.).
- A reload is invoked.

2.2.2 Backup Configuration

NOTE: Prerequisite: The system is properly configured as main system.

To support the backup and restore processes for the Disaster Recovery feature, the HiPath Backup & Restore (HBR) application replicates the software (including RMX and Unix updates) and the configuration data from the main system to the disaster recovery (standby) system.

As a rule, the backup takes place automatically, but it can also be initiated manually.

The replication process includes:

- RMX software + RMX data (including patches).
- Unix software and the Unix configuration data.

To include all software (including patches) and configuration data, the backup type „Disaster Recovery“ and the archive type “DR Backup Server“ have been defined.

Backup type „Disaster Recovery“

Backup type „Disaster Recovery“ contains the following data:

- Output of dump-aps code
- Output of dump-aps db
- Unix data backup
- Patch list
- SWT slice (Unix code)

Archive type „DR Backup Server“

Any Windows or Unix server can be used as the „DR Backup Server“. For HBR, it must work as a file server and so must support FTP In addition to dedicated file servers in the IT infrastructure, a HiPath 4000 Manager or the main system ADP can also be used as the backup server.

NOTE: If you want to use as backup directory **/.AS/BACKUP/IPDA** you should use for security reasons as ftp login „apeftp“.

The type „DR Backup Server“ archive can only contain one „Disaster Recovery“ type backup set. Other types of backup sets (data, system or logical) are not permitted.

The HBR of disaster recovery (standby) system scans a configured and activated DR backup server every 10 minutes, as long as the system is in disaster recovery (standby) mode. If a new completed backup is found, the data is transferred to the local hard disk. The restore operation begins after the transfer has completed.

The restore operation cannot be stopped and cannot be reversed.

To minimize the data traffic on the LAN/WAN, only the data that has changed since the last backup will be transferred to the DR backup server.

Basic conditions regarding timing

A backup can only be carried out when the DR backup server is free, i.e. not currently blocked by restore processes.

The interval between two scheduled backups must therefore be sufficient to allow the backup and restore processes of disaster recovery (standby) system to be carried out.

The time required is determined by the data volume to be transported and the available transmission bandwidth. The maximum data volume (in the case of a system maintenance release) is estimated at 100 MB. The average size will be less than 10% of the maximum.

The start time for the backup also determines indirectly the content of the database.
For example, if the customer usually activates fixed call forwarding on the telephone and if the backup is performed outside business hours, the saved database will contain the activated call forwarding settings.
But if a problem arises during the day, which initiates emergency mode, it will be initiated with the saved call forwarding settings.

1. Administration of disaster recovery (DR) backup server in HiPath 4000 Assistant

   Software Management > Backup & Restore > DR Backup Server

   or

   Software Management > Disaster Recovery > Configuration > Section **DR Backup Server** > Button **Configure**

   In both cases the **Backup & Restore** application is started.

   The configuration is done like a normal backup configuration. For more information please refer to HiPath 4000 Assistant/Manager V4, Backup and Restore, Administrator Documentation, Chapter 2, Administration Backup Server (see http://apps.g-dms.com:8081/techdoc/en/P31003H3440M1130176A9/HBR_Functionality31.html).

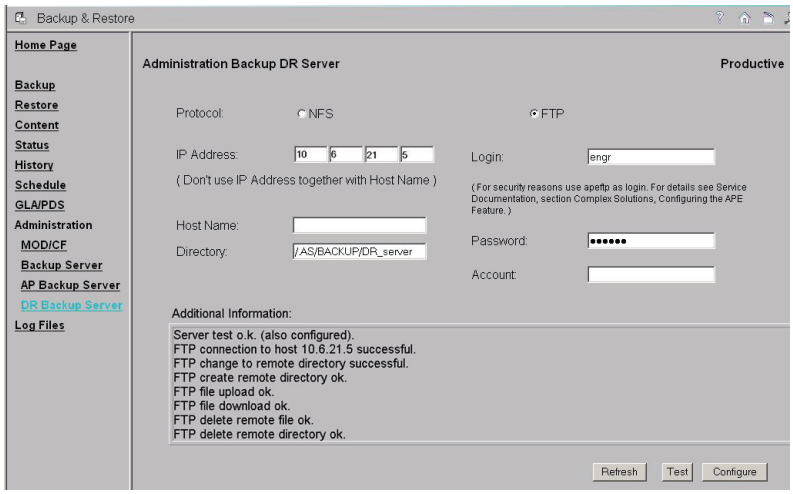

Figure 8 Backup server configuration (main system)

2. Schedule the data Disaster Recovery backup (DDR type) in HiPath 4000 Assistant

   Software Management > Backup & Restore > Schedule

   The configuration is done like a normal schedule configuration.

   Please be aware that AP backup is also scheduled within AP emergency configuration. The time of AP backup and DR backup must not overlap.

   For more information please refer to HiPath 4000 Assistant/Manager V4, Backup and Restore, Administrator Documentation, Chapter 2, Schedule (see http://apps.g-dms.com:8081/techdoc/en/P31003H3440M1130176A9/HBR_Functionality27.html).

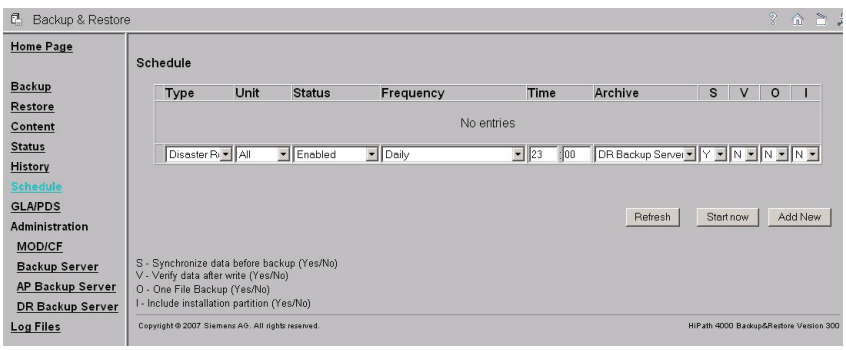

Figure 9 Schedule configuration for backup (main system)

2.2.3 Disaster Recovery Configuration Page after Successful Configuration

After successful configuration of the main system the configuration page looks like the following.

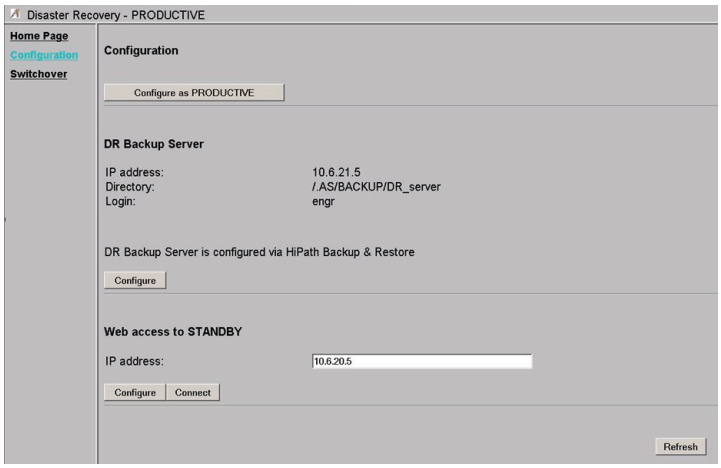

Figure 10 Configuration page of disaster recovery after successful configuration

2.3 Disaster Recovery (Standby) System

2.3.1 Configuration as Disaster Recovery (Standby) System

1. Configure your system as main system (see Section 2.2.1, “Configuration as Main System”).
2. For administration purposes configure **manually** the IP address of HiPath 4000 Assistant. This must be the IP address of the disaster recovery system and is another IP address than the one of the main system.

   Base Administration > Unix Base Administration > LAN Card Configuration
3. Now switch over from main system to disaster recovery system.

   Software Management > Productive Switch > Switch Over > button **Switch to STANDBY**

   The switch over will configure both RMX side and HiPath 4000 Assistant side and a reload of the system is invoked.

   This means:

   - The disaster recovery flag is set to **YES** (AMO CPCI, **DISREC=YES**). You can check the status with AMO CPCI, **DISREC=YES** and HiPath 4000 Assistant **Disaster Recovery**. Whith this configuration of the disaster recovery flag the IPDA LAN interface won’t be initialized and a connection to the access points cannot be set up.

- Some processes are stopped (e.g. Performance Management, Configuration Management, etc.).
- A reload is invoked.

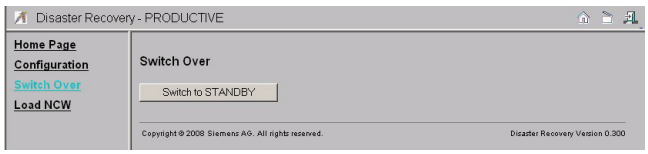

Figure 11 *Switch over to disaster recovery (standby) server for the first time*

2.3.2 Backup Configuration

NOTE: Prerequisite: The system is properly configured as disaster recovery (standby) system.

Now you can configure DR Backup server. This is the FTP server, from where the backup will be downloaded. That means that main and standby systems must use the same DR backup server.

Do not enable **Automatic restore disable**. Then HBR automatically starts the scanning of the DR Backup Server for new backups. If so, the backup is downloaded and then restored.

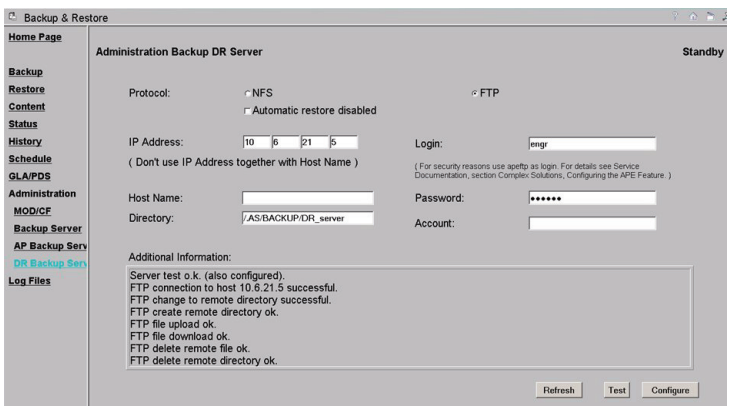

Figure 12 *Backup server configuration (standby system)*

Because of the fact that the automatic restore is disabled, you can start the data DR Recovery manually.

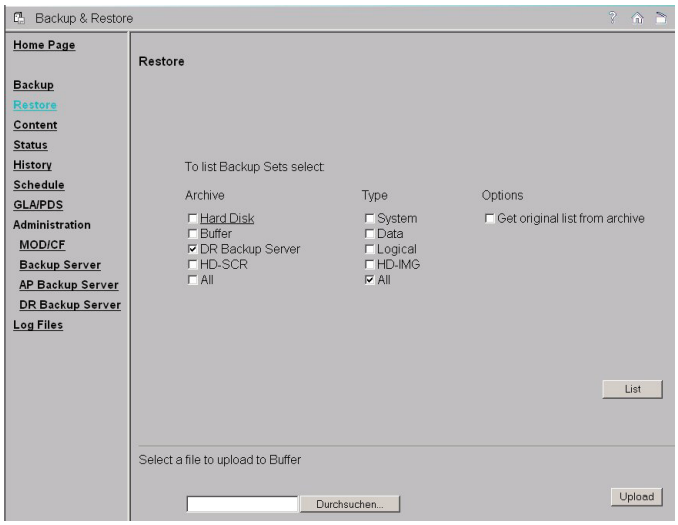

Figure 13 Manually start the restore from DR backup server (standby system) - Step 1

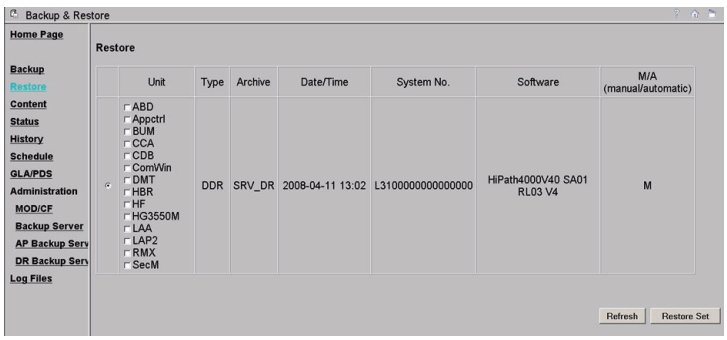

Figure 14 Manually start the restore from DR Server (standby system) - Step 2

2.4 Web Access to Complementary System

With this feature you can easy access the complementary system. From main system you can quickly access the disaster recovery (standby) system and from disaster recovery (standby) system you can quickly access the main system.

Example: Configuration of the „Web Access to STANDBY“

Configuration is done via **Software Management > Disaster Recovery > Configuration** > Section **Web Access to Standby**.

Enter the **IP address** of the disaster recovery (standby) system and press **Configure**.

Now you can establish a connection to the disaster recover (standby) system:

- **Software Management > Disaster Recovery > Web Access to Standby** or

- **Software Management > Disaster Recovery > Configuration >** section **Web Access to Standby >** button **Connect**.

Figure 15 *Web access to disaster recovery (standby) system configuration in main system*

NOTE: The configuration for the **WEB access to PRODUCTIVE** is done ion the same way but on the disaster recovery (standby) system.

2.5 Time Synchronization Between the Main System and the Disaster Recovery (Standby) System

There should be an external time server (currently different from main and disaster recovery (standby) system) that both the main and the disaster recovery (standby) systems are connected to syncronize time and date. This should be provided in order to overcome problems that could occur with codewords, SPE and other components that are time based.

It is important that the main and the disaster recovery (standby) systems have the exact time and date configuration in case of a switch over. The external time server can be configured using the Unix Base Administration:

- Log on to Hipath 4000 Assistant
- **Base Administration > Unix Base Administration > Date/Time**
- Select the **Time Servers** tab and enter the IP **Address** of the external time server in the **Time Server Address** box and click the **Add** button.This is the external server that you would like the disaster recovery system to be syncronized with.

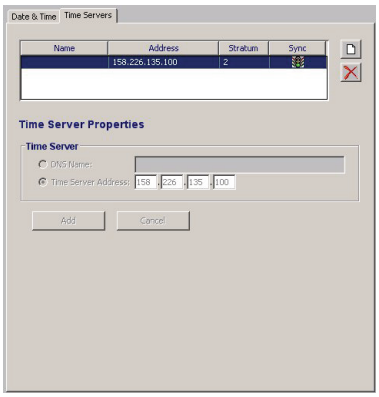

Figure 16 Time server configuration with Unix Base Application

- Select the **Date&Time** tab and click on the radio button **External (Full Network Time Protocol (NTP) operation)**. Select the Time Zone if needed and click on the **Modify** button.

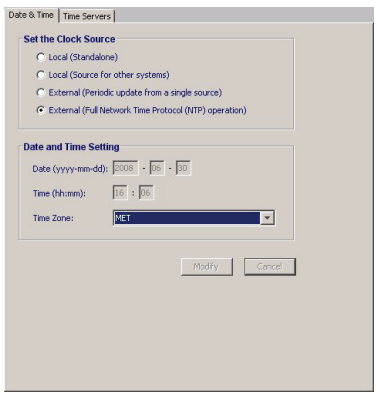

Figure 17 External clock configuration with Unix Base Application

- The configuration must be done on both systems and the same time server must be used for the main and the disaster recovery (standby) system.

3 Switch Over in Case of a Disaster

3.1 Switch Disaster Recovery (Standby) System to Main System

NOTE: Prerequisite: Main system is disconnect from IP/LAN network to avoid IP conflicts.

1. Check if the LAN cables have been connected to the disaster recovery (standby) system.
2. Perform switch over.

   Software Management > Disaster Recovery > Productive Switch > Switch Over

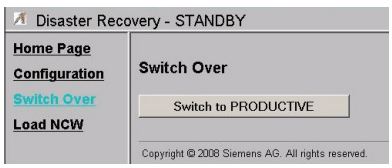

Figure 18 Switch over to productive mode

Following actions are automatically done:

- The disaster recovery flag is set to **NO.** You can check the status with AMO CPCI, **DISREC=NO** and HiPath 4000 Assistant application **Disaster Recovery**.
- The IP address of C-LAN is changed to IP address of original main system.
- Some processes are started (e.g. Performance Management, Configuration Management, etc.).
- A reload is invoked.

3.2 Re-Installation of the Main System and Switch Back to Main System

The main system hardware is available again.

The following steps have to be performed before executing the switch back:

1. Configure the main system in the first step as disaster recovery system (refer to Section 2.3.1, “Configuration as Disaster Recovery (Standby) System”.

NOTE: Don’t forget to change the IP address of HiPath 4000 Assistant!

---

2. Configure the Backup and perform a synchronization with the productive system (refer to Section 2.3.2, “Backup Configuration”). At least one synchronization must be done before perfroming the switch over.
3. Disconnect the disaster recovery system which is in productive mode from the IP/LAN network to avoide IP address conflicts.
4. Optionally activate Acces Point Emergency mode with AMO APESU).
5. Perform switch over for the main system as described in Section 3.1, “Switch Disaster Recovery (Standby) System to Main System”.

3.3 Switch Back Disaster Recovery System to Disaster Recovery Mode

---

NOTE: Prerequisite: Disaster recovery system is disconnect from IP/LAN network to avoid IP conflicts.

---

1. For administration purposes configure **manually** the IP address of HiPath 4000 Assistant.

   Base Administration > Unix Base Administration > LAN Card Configuration

2. Perform switch over to standby mode

   Software Management > Disaster Recovery > Productive Switch > Switch Over

Figure 19 Switch over to standby mode

After pressing the **Switch Over** button a message box appears:

To continue press **OK**.

Following actions are automatically done:

- The disaster recovery flag is set to **YES** (AMO CPCI, **DISREC=YES**). You can check the status with AMO CPCI, **DISREC=YES** and HiPath 4000 Assistant **Disaster Recovery**.
- Some processes are stopped (e.g. Performance Management, Configuration Management, etc.).
- A reload is invoked.

4 Load Network Codeword (NCW)

Generally there are two possibilities to add a code word to the system:

1. The code word is directly added to system by the service personnel. The service personnel is then responsible for the validity of the code word.
2. Systems are connected to the HiPath 4000 Manager and the LMT on the HiPath 4000 Manager takes care about the adding and periodic refreshing of the code word.

The **Load NCW** function deals with the second possibility.

Because of the fact that only the main system is registered at the HiPath 4000 Manager the network code word can only be refreshed through LMT on the main system. For the disaster recovery (standby) system the network code word is loaded via the function **Load NCW**. The customer gets the network code word from the service tchnician. After configuring this NCW the LMT on the disaster recovery (standby) system periodically generates the new NCW, which has only a validity of 5 days.

LMT generates the NCW only if the system runs in as disaster recovery system (standby mode). After the switch over of the disaster recovery system the LMT does not generates the NCW anymore because the system is now in productive mode and will get the NCW from HiPath 4000 Manager.

For more information on LMT please refer to the HiPath 4000 Manager V4, License Management Tool - Access Management, Administrator Documentation (http://apps.g-dms.com:8081/techdoc/en/P31003H3440M1110176A9/index.htm).

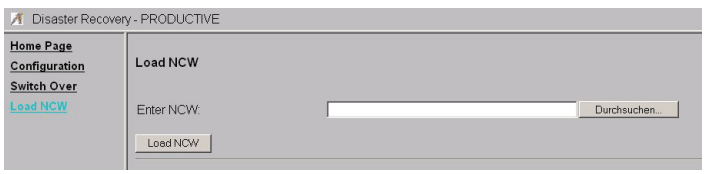

Figure 20 Load network code word for disaster recovery (standby) system

List of Tables

List of Figures

Index