

Documentation

HiPath 4000 V5 IP Solutions - IPDA & APE

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

Copyright © Siemens Enterprise
Communications GmbH & Co. KG 2009
Hofmannstr. 51, 80200 München

Siemens Enterprise Communications GmbH & Co. KG
is a Trademark Licensee of Siemens AG

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

The information provided in this document contains
merely general descriptions or characteristics of
performance which in case of actual use do not
always apply as described or which may change as
a result of further development of the products. An
obligation to provide the respective characteristics
shall only exist if expressly agreed in the terms of
contract. Availability and technical specifications are
subject to change without notice.

OpenScape, OpenStage and HiPath are registered
trademarks of Siemens Enterprise
Communications GmbH & Co. KG.

All other company, brand, product and service
names are trademarks or registered trademarks of
their respective holders.

Service Manual HiPath 4000 V5 - IP Solutions - IP Distributed Architecture (IPDA) and Access Point Emergency (APE) - Contents

| | |
|---|-----------|
| 1 IPDA Feature Description | 7 |
| 1.1 Scalable Increase in System Capacity | 8 |
| 1.2 Distributed Circuit Switching | 9 |
| 1.3 Survivability for Signaling and Payload | 9 |
| 1.4 Additional Features | 9 |
| 1.5 Call Scenarios | 10 |
| 1.5.1 Internal Access Point Call | 11 |
| 1.5.2 Call Between Two Access Points | 12 |
| 1.5.3 Call Between an Access Point and the Central System | 13 |
| 1.5.4 Trunk access/networking | 14 |
| 1.5.5 Survivability | 15 |
| 1.6 Different Time Zones (DTZ) | 16 |
| 2 Access Point Emergency Feature Description | 18 |
| 2.1 Previous Survivability Function (HiPath 4000 V1.0) | 18 |
| 2.2 Access Point Emergency Implementation Scenarios | 19 |
| 2.3 Access Point Emergency and Signaling Survivability | 22 |
| 2.4 Survivability Unit | 23 |
| 2.5 Allocating Access Points to a Survivability Unit | 24 |
| 2.6 Switchover in Emergency Mode | 24 |
| 2.7 Reverting to Normal Operation | 25 |
| 2.8 Configuration Data | 26 |
| 2.9 Transferring New System Releases and Patches | 27 |
| 2.10 Connection Between Subsystems (Islands) | 27 |
| 2.11 Time Synchronization | 28 |
| 2.12 Feature Licensing | 29 |
| 2.13 Application Support in Emergency Mode | 29 |
| 3 HiPath 4000 in the Customer LAN | 31 |
| 3.1 LAN Interfaces for the Processor Modules | 31 |
| 3.1.1 HiPath 4000 with DPC5 Processors | 31 |
| 3.1.2 HiPath 4000 with DSCXL Processors | 32 |
| 3.2 Connecting the Local Craft Terminal (LCT) at the Access Point | 32 |
| 3.3 Checking the IP Addresses Used | 32 |
| 3.4 AP 3700 IP with Survivability Unit in the Customer LAN | 34 |
| 4 Configuring the IPDA Feature | 37 |
| 4.1 Configuring the HiPath 4000 LAN Segment | 38 |
| 4.2 Configuring an Access Point | 57 |
| 4.2.1 Configuring a "Networked" Access Point | 58 |
| 4.2.2 Configuring a "Direct Link" Access Point | 68 |
| 4.2.3 Changing Access Point Parameters with the AMO STMIB | 80 |
| 4.2.4 Deleting an Access Point | 81 |
| 4.2.5 Local Configuration of an Access Point | 83 |
| 4.2.6 Reference Clock in Access Point | 86 |

| | |
|--|------------|
| 4.2.7 Loading New Loadware on a HiPath HG 3575 | 87 |
| 4.2.8 Updating Access Point Loadware during an RMX Upgrade (New Fix Release/Minor Release) | 89 |
| 4.2.9 Information on Exchanging HiPath HG 3575 Boards | 91 |
| 4.2.10 Information on the 19" HiPath AP 3500 IP Access Point | 92 |
| 4.2.11 Information on the 19" HiPath AP 3700 IP Access Point. | 94 |
| 4.3 Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 System | 96 |
| 4.4 Configuring Special Routes | 101 |
| 4.4.1 Special Routes Between Access Points | 102 |
| 4.4.2 Special Routes between Access Point and HiPath 4000 LAN Segment. | 104 |
| 4.5 Configuring Signaling Survivability | 112 |
| 4.5.1 How is the Fault Detected? | 113 |
| 4.5.2 What is Used as an Alternative Route for Signaling? | 115 |
| 4.5.3 Generation. | 117 |
| 4.5.4 Is Signaling Survivability Currently Active? (DIS-UCSU). | 122 |
| 4.5.5 Configuring the Modem | 123 |
| 4.5.6 Configuring the Router | 125 |
| 4.5.6.1 Signaling Flow Survivability for "Networked" Access Points | 125 |
| 4.5.6.2 Signaling Flow Survivability for "Direct Link" Access Points | 126 |
| 4.5.6.3 Signaling Survivability with WAML Replacement. | 128 |
| 4.5.6.4 External ISDN Router as the Survivability Router | 130 |
| 4.6 Configuring Quality Monitoring for the Signaling Connection over IP | 132 |
| 4.6.1 Restriction of the Available Signaling Bandwidth (Traffic Shaping). | 132 |
| 4.6.2 Monitoring the Runtime for Signaling Messages (Round Trip Delay) | 134 |
| 4.6.3 Monitoring Message Throughput. | 136 |
| 4.6.4 Advanced Criteria for Signaling Survivability. | 137 |
| 4.6.5 Output of Statistical Information on the Signaling Connection | 139 |
| 4.6.6 Error Messages from Quality Monitoring for the Signaling Connection over IP | 140 |
| 4.6.6.1 F8289 - Output of Statistics Data. | 140 |
| 4.6.6.2 F8290 - Net Weakness Start Message Runtime Exceeded. | 142 |
| 4.6.6.3 F8290 - Net Weakness Start Message Throughput Undershoot. | 143 |
| 4.6.6.4 F8291 - Net Weakness End. | 143 |
| 4.6.6.5 F8292 - Bandwidth Requirement Exceeds Limit | 144 |
| 4.6.6.6 F8293 - Bandwidth Required Back Below Limit. | 144 |
| 4.7 Configuring Source Dependent Routing | 145 |
| 4.8 Configuring Payload Survivability | 149 |
| 4.8.1 When is Payload Survivability Used? | 150 |
| 4.8.2 Possible Features | 153 |
| 4.8.3 How is Payload Survivability Configured? | 156 |
| 4.8.4 Payload Survivability in HiPath 4000 Networks. | 165 |
| 4.9 Configuring Subscriber, CO/Tie Trunk Circuits in Access Points | 168 |
| 4.10 External Music on Hold | 176 |
| 4.11 Information on CMI | 181 |
| 4.12 IP Address Changes. | 182 |
| 4.12.1 Change of Address in a Network Segment to which Access Points are Connected. | 182 |
| 4.12.2 Changing the Address of the Survivability Network. | 185 |
| 4.12.3 Changes in the HiPath 4000 LAN Segment | 185 |
| 5 Configuring the APE Feature (Access Point Emergency) | 192 |
| 5.1 Configuring or Modifying a CC-AP in HiPath 4000 | 193 |
| 5.2 Deleting a CC-AP in HiPath 4000 | 195 |
| 5.3 Configuring or Modifying an Emergency Group | 195 |

| | |
|--|------------|
| 5.4 Deleting an Emergency Group | 199 |
| 5.5 Configuring Access Points for AP Emergency | 200 |
| 5.6 Examples for Determination of Weights | 202 |
| 5.7 Removing Access Points from the AP Emergency Configuration | 204 |
| 5.8 Deleting the Entire AP Emergency Configuration | 204 |
| 5.9 Configuring the Display for AP Emergency on the optiSet/optiPoint | 205 |
| 5.10 Defining the Switchover Delay | 205 |
| 5.11 Querying the Connection Data | 207 |
| 5.11.1 Querying the Connection Data via Configuration Management | 207 |
| 5.11.2 Querying the Connection Data via AMO | 208 |
| 5.12 Administration Switchover of APs | 210 |
| 5.12.1 Administration Switchover of APs via Configuration Management | 210 |
| 5.12.2 Administrator Switchover of APs via AMO | 210 |
| 5.13 Time Synchronization Between the Central System and CC-AP | 212 |
| 5.14 HiPath 4000 Backup & Restore | 216 |
| 5.14.1 Configuring an AP Backup Server with HiPath 4000 Backup & Restore | 217 |
| 5.14.2 Creating a Schedule for the Backup | 219 |
| 5.14.3 Performing the First Backup | 221 |
| 5.14.4 Using HBR For More Extensive Changes in the System | 221 |
| 5.14.5 Checking the Regular Activities of HBR | 222 |
| 5.15 Initial Startup of the CC-AP | 223 |
| 5.15.1 Part Number of the Current APS on the HiPath 4000 Central System | 223 |
| 5.15.2 Creating an MO Disk / HDCF for the First Startup of the CC-AP | 224 |
| 5.15.3 Starting the CC-AP | 224 |
| 5.15.4 Copying the Program System from the MO Disk/HDCF to the Hard Disk | 225 |
| 5.15.5 Reloading the CC-AP - Initial Unix Installation | 225 |
| 5.15.6 RMX Configuration of the CC-AP | 226 |
| 5.15.7 Unix Configuration on the CC-AP | 227 |
| 5.15.7.1 Configuring the IP Address in the CUSTOMER Network | 227 |
| 5.15.7.2 Configuring the Default Router | 228 |
| 5.15.7.3 Configuring Time Synchronization | 228 |
| 5.16 HiPath Backup Restore Configuration on the CC-AP | 232 |
| 5.16.1 Preparation | 232 |
| 5.16.2 Generating the GLA | 232 |
| 5.16.3 Configuring the AP Backup Server on the CC-AP | 233 |
| 5.16.4 Configuring a Routine Configuration Data Backup to Hard Disk | 235 |
| 5.16.5 Creating a Routine Backup on MO Disk/HDCF | 237 |
| 5.17 Upgrading the AP Emergency Computer (New Fix Release/Minor Release) | 239 |
| 5.18 Verification and Acceptance of the AP Emergency Configuration | 239 |
| 6 Load Calculation | 241 |
| 6.1 Load Calculation for Access Points | 245 |
| 6.2 Load Calculation for a HG 3500 | 252 |
| 6.3 Calculation Basis - Configuring Payload Packets | 259 |
| 6.3.1 Configuring Ethernet MAC Frames | 259 |
| 6.3.2 Configuring IP Frames | 260 |
| 7 Local Access Point Administration at CLI via Terminal | 261 |
| 7.1 Networked access point | 262 |
| 7.2 Direct link access point | 263 |
| 7.3 Additional settings for the initial startup | 265 |
| 7.4 Assignment of parameter names in LW-CLI to the AMO parameters | 266 |

| | |
|--|------------|
| 8 Spreadsheets - IPDA Configuration..... | 269 |
| 9 LCT configuration | 280 |
| 9.1 Configuring the PPP Connection to HG 3575 under Windows 2000 | 280 |
| 9.1.1 Installing the NULL Modem | 280 |
| 9.1.2 Installing the PPP Connection..... | 286 |
| 9.2 Configuring the PPP Connection to HG 3575 under Windows XP..... | 299 |
| 9.2.1 Installing the NULL Modem | 300 |
| 9.2.2 Installing the PPP Connection..... | 301 |
| 9.3 Notes on Using the PPP Connection | 303 |
| 10 Information for network administrators | 304 |
| 10.1 Central Processor | 304 |
| 10.2 HG 3500 Voice Gateway | 304 |
| 10.3 Access Points with HG 3575 | 305 |
| 10.4 Survivability Unit for AP Emergency | 309 |
| 10.5 Redundant LAN Interface | 310 |
| 11 IPDA Wizard | 313 |
| 11.1 Functions | 313 |
| 12 Short description how to install an AP Emergency (IPDA) | 317 |
| 12.1 Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP 18) | 317 |
| 12.1.1 Steps of installation in the HiPath 4000..... | 319 |
| 12.1.2 Steps to configure the Access Points 17 and 18..... | 328 |
| 12.1.3 Verification and Acceptance of the AP Emergency Configuration..... | 341 |
| 12.2 Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access Point (AP 18). | 342 |
| 12.2.1 Configuration steps in the HiPath 4000 V2.0..... | 344 |
| 13 FAQs - Frequently Asked Questions | 353 |
| Index | 367 |

1 IPDA Feature Description

HiPath 4000 offers the possibility of distributing access points across an IP network. These access points are shelves which accommodate the standard HiPath 4000 access modules. The subscriber line circuits at the access points are handled precisely as if they were linked directly - as has been customary in the past - to a HiPath 4000 switch. Administration of all components distributed via IP is also realized as **one** system via an access point of the HiPath 4000 system.

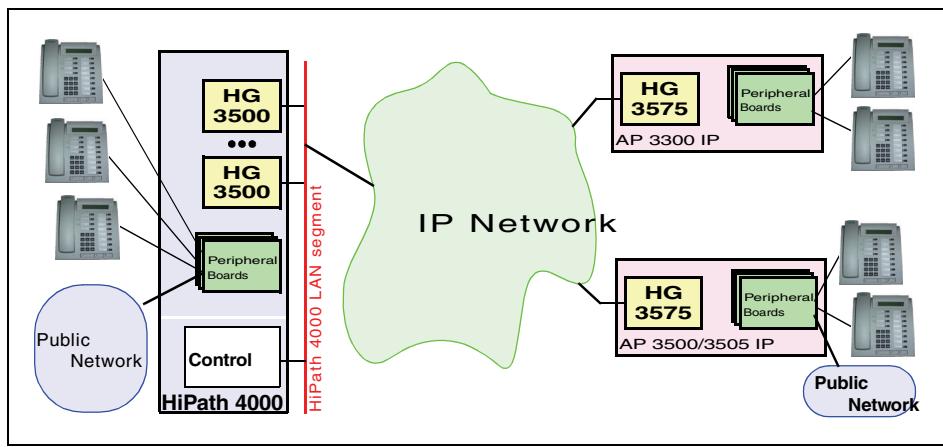


Figure 1 Overview of architecture

The “IP distributed architecture“ comprises the following main components:

- HiPath 4000 The communication server, which also controls all components of the “IP Distributed Architecture“. The rich volume of call processing features is thus also available to the “IP Distributed Architecture“.
- HiPath HG 3500 This IP gateway module allows payload connections between subscriber line/CO and tie trunk circuits in the central part of the HiPath 4000 system and subscriber/CO and tie trunk circuits in the distributed access points.
- IP Access Points There are two types of IP-based access points
- HiPath AP 3300 IP This traditional Flexpack shelf with IP integration offers 16 slots for HiPath 4000 peripheral modules
- HiPath AP 3500 IP This new 19“ shelf (3 units high), which can be mounted in a 19“ rack, allows inexpensive configurations for small locations. As a basic box, it offers 3 slots for HiPath 4000 peripheral modules. The number of slots can be increased to 7 with an AP 3505 IP expansion box (3 units high). Both the HiPath AP 3500 IP and the HiPath AP 3505 IP expansion box can be equipped with a redundant power supply.

IPDA Feature Description

Scalable Increase in System Capacity

- HiPath AP 3700 IP This new 19" shelf (10 units high), which can be mounted in a 19" rack, features nine slots for HiPath 4000 peripheral boards. The frame comes with three PSU modules which are operated in a 2+1 redundancy configuration.
It can also take over autonomous control in emergencies within the context of the Access Point Emergency feature.

Both types of access point are equipped with a HiPath HG 3575 connection module, which establishes the connection to the IP infrastructure (10/100BT).

The IP-based access points allow the use of the majority of current and future modules which can be operated in classic HiPath 4000 shelves.

The HiPath HG 3500 and HG 3575 modules are each equipped with a 10/100BT Ethernet connection for connecting to the IP network.

1.1 Scalable Increase in System Capacity

HiPath 4500 supports up to 83 access points linked via IP (AP 3300 IP, AP 3500/3505 IP or AP 3700 IP), in addition to a maximum of 15 directly linked shelves (AP 3300 or AP 3700).

HiPath 4300 supports up to 40 access points linked via IP (AP 3300 IP, AP 3500/3505 IP or AP 3700 IP), in addition to a maximum of three directly linked shelves (AP 3300 or AP 3700).

Thus, the maximum number of digital subscriber line circuits in a system can be increased to 12000.

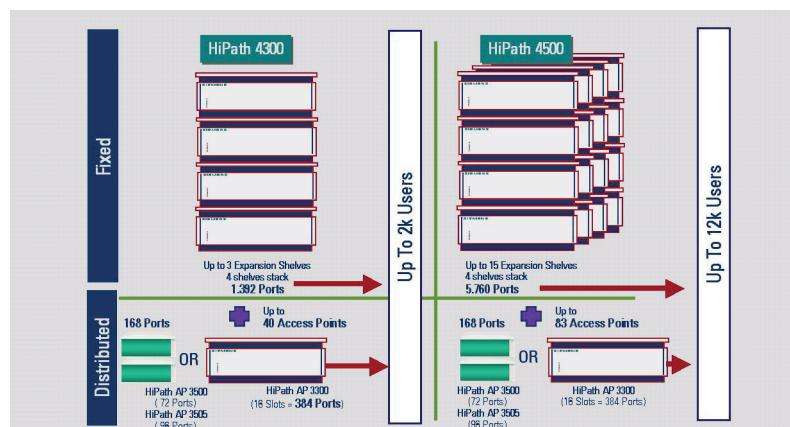


Figure 2

Scalable increase in system capacity

1.2 Distributed Circuit Switching

With HiPath 4000, the circuit switching of the payload (B channels) is not limited to the central switching network

- Calls within IP-based access points are switched to a local TDM switching network directly and, consequently, without runtime in the IP network. The switching network on the HiPath HG 3575 module has a capacity of 256 channels.
- Calls between different IP-based access points are switched in the IP network.
- Calls which go beyond IP-based access points are switched both in the IP network and in the central HiPath 4000 system.

1.3 Survivability for Signaling and Payload

Survivability for signaling and payload ensures that HiPath 4000 also offers the greatest availability in distributed operation. The public telephone network can be used as an alternative route in the event of an IP network failure or if the IP network temporarily fails to provide the requisite quality for voice transmission.

Payload

Survivability for payload uses regular trunk circuits in the public telephone network. The route for payload survivability is also selected automatically as a spillover route if the entire capacity of the HG 3575 is already in use in the IP network.

Note: For information about feature restrictions with payload survivability, see [Section 4.8, “Configuring Payload Survivability”, on page 149](#)

Signaling

Survivability for signaling ensures that an access point can be controlled centrally by the HiPath 4000 at all times. If the direct route for signaling via the IP network fails, an alternative route is established via a modem route.

1.4 Additional Features

- High voice quality

On account of longer voice signal delays caused by the system in the IP network, voice quality will be impaired by echo unless this is removed prior to transmission. The HiPath HG 3500 and HG 3575 modules therefore feature an integrated echo canceller.

IPDA Feature Description

Call Scenarios

Lower bandwidth requirements

If voice is transmitted via IP in uncompressed form (pursuant to G.711), the bandwidth requirement is greater than in the case of ISDN on account of the packaging in the IP protocol.

If less bandwidth is to be occupied, the voice signal can be compressed. HiPath HG 3500 and HG 3575 offer optional compression pursuant to the G.729A standard (only 8 Kbps, instead of 64). Furthermore, additional bandwidth can be saved by suppressing voice pauses. Silence suppression suppresses the transmission of silence on the line. (G.729AB, or G.711 Annex 2)

- Support for Quality of Service in the IP network through prioritization

HiPath 4000 IP distributed architecture supports prioritization in the IP network on the basis of the following standards:

- IEEE 802.1 p/q (VLAN Tagging) on Layer 2
- IETF RFC 2474 (DiffServ) on the IP Layer
- Transport capacity in the IP network

HiPath HG 3500 and HG 3575 can transmit up to 120 B channels simultaneously over the IP network regardless of the hardware and configuration in use (see "HiPath Gateways HG 3500 and HG 3575, [Section 3.6, “B Channels”](#)").

- Support of network management on the basis of SNMP

HiPath HG 3500 and HG 3575 support network management on the basis of the SNMP protocol. Statistical data from the applicable standard MIBs and additional data from proprietary MIBs can be queried.

- Redundant LAN Interface

For increased resilience, IPDA V2.0 boards HG 3500 and HG 3575 should be connected with two LAN cables to different switches (please refer to [Section 10.5, “Redundant LAN Interface”](#)).

1.5 Call Scenarios

In order to gain a better understanding of the call processing procedures and their distribution across the components of the IP distributed architecture, a couple of typical call scenarios are described below. The original graphics are available for sales training as an animated PowerPoint presentation.

1.5.1 Internal Access Point Call

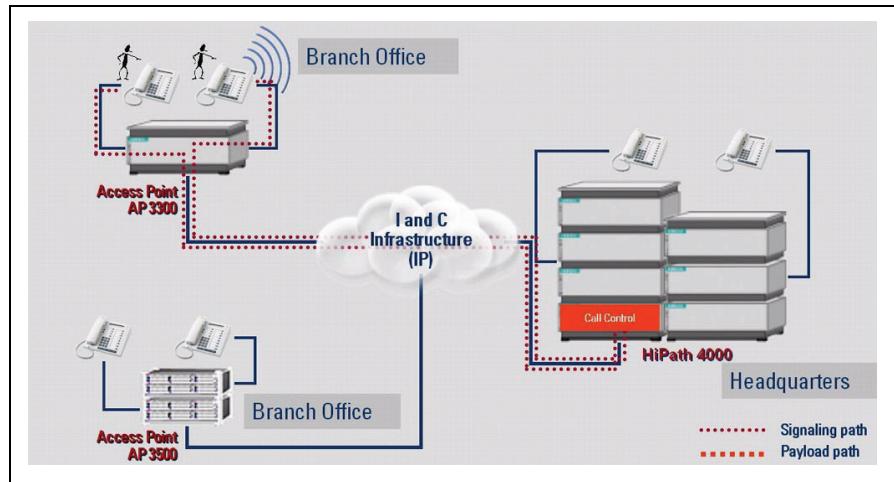


Figure 3 Signaling for an internal access point call

Signaling from and to the connected telephones is always transmitted over the IP network to the call processing infrastructure in the HiPath 4000 central system, and from there back again.

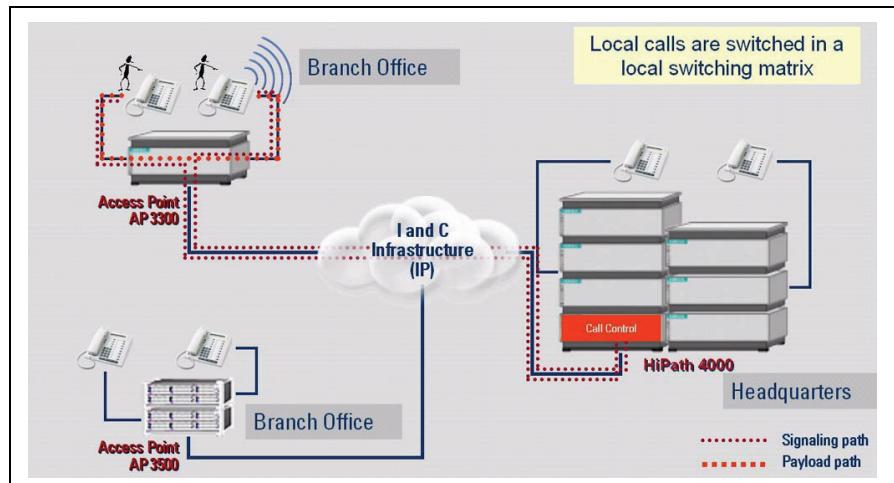


Figure 4 Voice link (payload) for an internal access point call

The central call processing infrastructure establishes the voice link and makes all features available. In this case, the voice link is switched within the access point in the TDM-based switching network of the HG 3575 module. This means that no payload is generated in the IP network and none of the channels of the transport capacity from the access point to the IP network are occupied.

1.5.2 Call Between Two Access Points

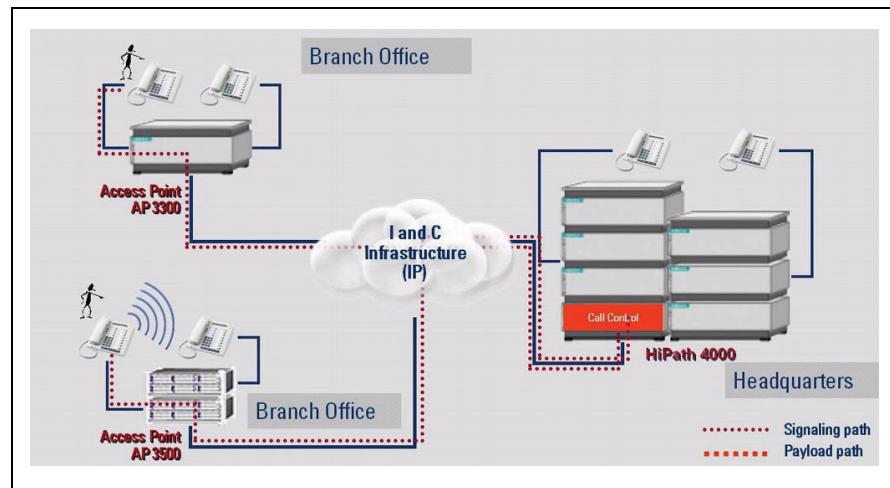


Figure 5 Signaling for an access point \leftrightarrow access point call

Signaling from and to the connected telephones is always transmitted over the IP network to the call processing infrastructure in the HiPath 4000 central system, and from there back again.

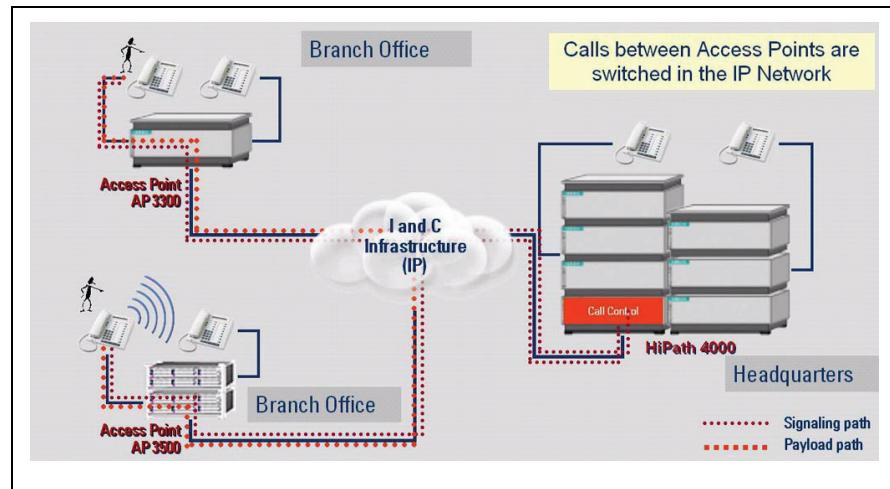


Figure 6 Voice link (payload) for an access point \leftrightarrow access point call

The central call processing infrastructure establishes the voice link and makes all features available. In this case, the voice link between the two access points is switched in the IP network with the aid of the HG 3575 modules. Each of the access points occupies one channel of the available transport capacity to the IP network.

1.5.3 Call Between an Access Point and the Central System

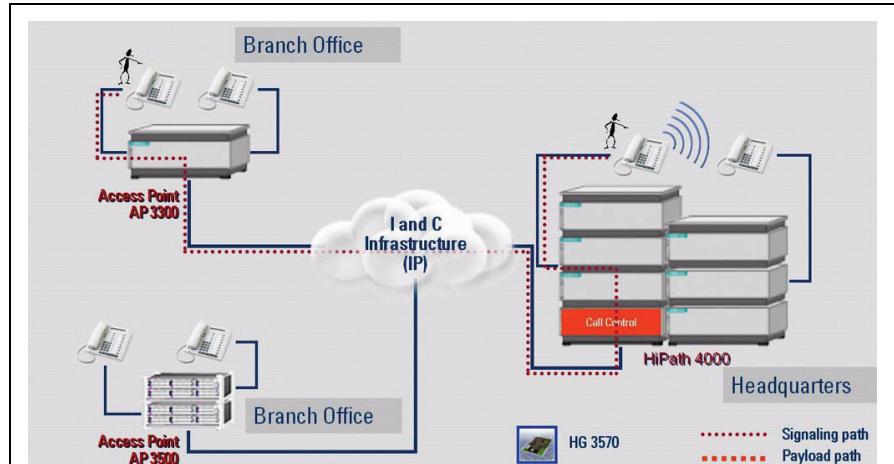


Figure 7 Signaling for an access point \leftrightarrow central system call

Signaling from and to the connected telephone in the access point is always transmitted over the IP network to the call processing infrastructure in the HiPath 4000 central system, and from there back again.

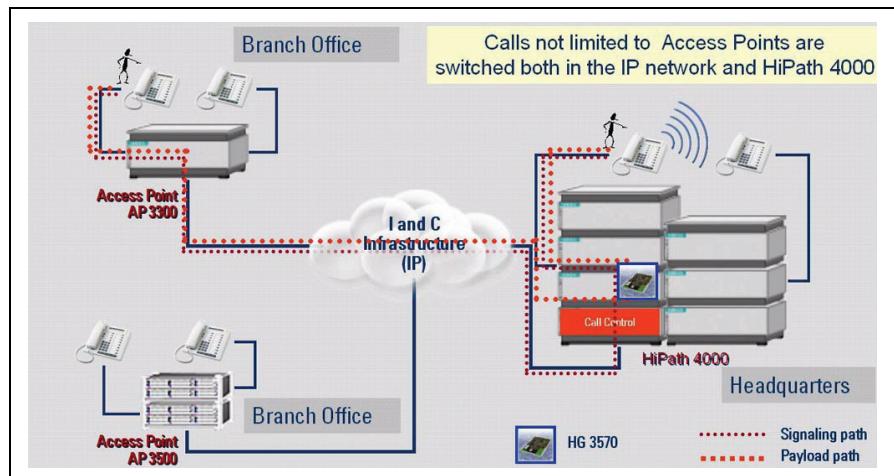


Figure 8 Voice link (payload) for an access point \leftrightarrow central system call

The central call processing infrastructure establishes the voice link and makes all features available. The voice link from the access point is switched to the IP network with the aid of the HG 3575 module. The HG 3500 module functions as a gateway and converts the IP data stream back into a PCM data stream that can be processed by the central system. This data stream is transferred to the connected subscriber within the central system. The call is therefore switched in both the IP network and in the HiPath 4000 central system. The access point and the gateway module each occupy one channel of the available transport capacity to the IP network.

1.5.4 Trunk access/networking

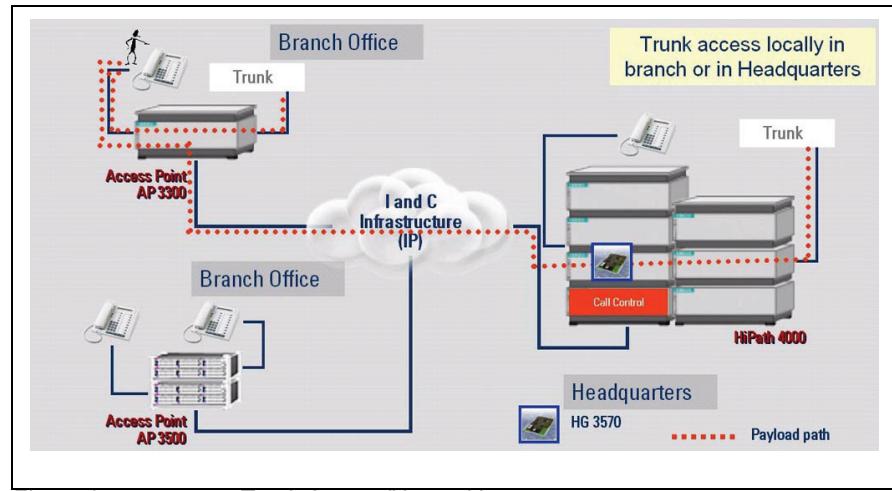


Figure 9 Trunk Access/Networking

Local trunk access can also be set up in an access point. The least cost routing function of the HiPath 4000 decides which trunk access to use based on the subscriber's location.

1.5.5 Survivability

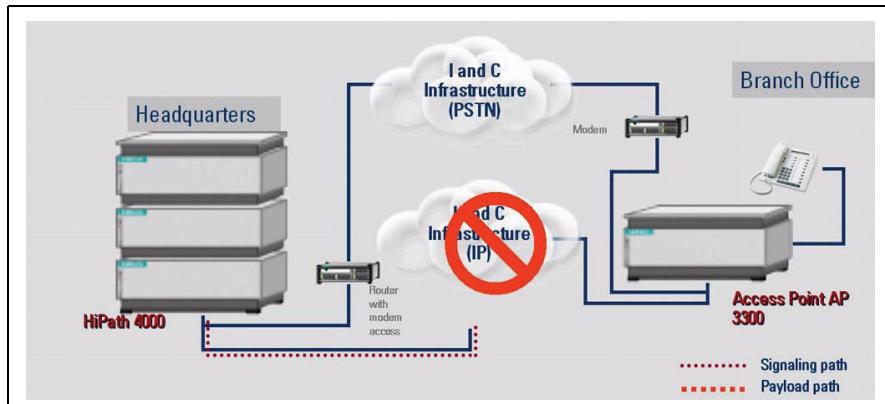


Figure 10 Survivability: failure in the IP network

If the IP connection from an access point to the central system fails, there can be no interaction between the access point and the central system. Messages from the terminal devices and trunks in the access point are temporarily buffered on the HG 3575, while messages from the central system are buffered in the central processor. If the duration of the failure exceeds a definable limit, the access point performs a reset, thereby disconnecting all calls.

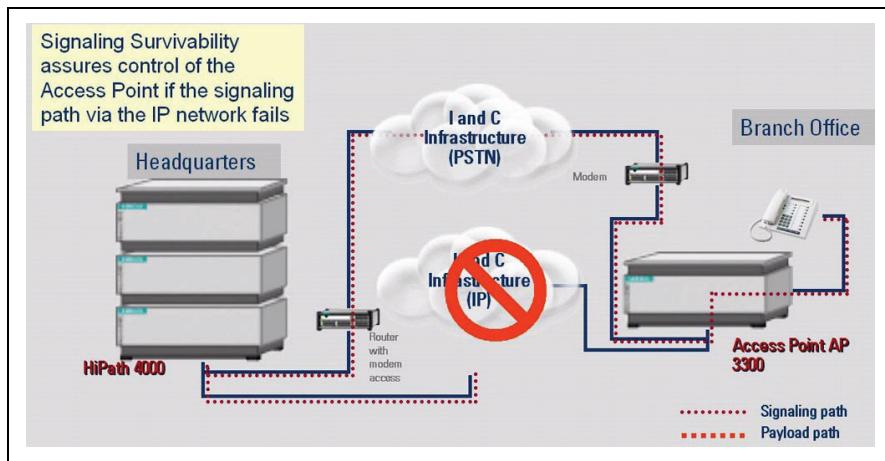


Figure 11 Signaling survivability: signaling via PSTN

With signaling survivability, an *alternative route* for signaling via the ISDN network (PSTN) is set up as soon as a fault in the IP path is detected. The messages are then routed via a PSTN router to the central system (for example, router with IP --> S2 or STMI2/4 board with WAML function) and an ISDN modem on the access point. The signaling messages are sent via this alternative path once it is established (approx. 30 ... 60 seconds). This ensures that none of the messages that may be in a backlog are lost.

IPDA Feature Description

Different Time Zones (DTZ)

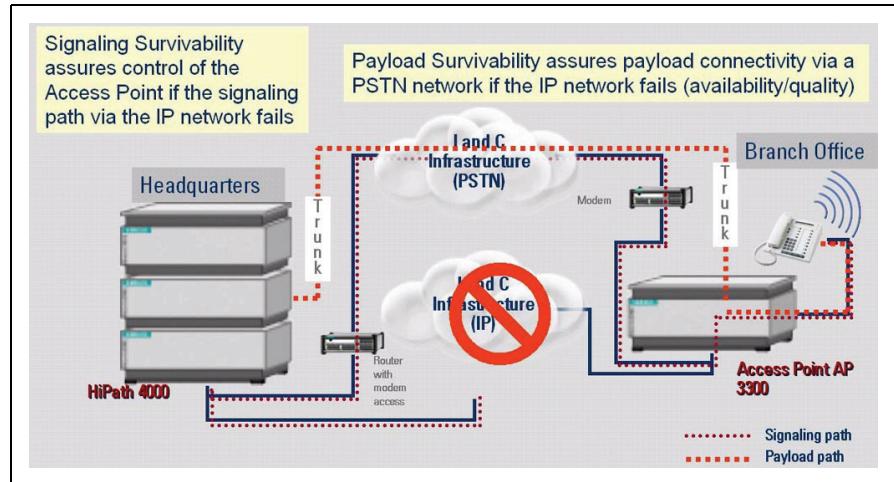


Figure 12 Payload survivability: alternative route for the payload via PSTN

If the payload path (between access points or between access points and the central system) fails in addition to the signaling path, payload survivability allows *internal system* calls to be routed via the CO as an alternative. The HiPath 4000 in effect “calls itself” and establishes an internal call between different parts of the system.

1.6 Different Time Zones (DTZ)

The “Different Time Zones (DTZ)“ feature is used in situations when an IPDA shelf or access point (AP-IP) or HFA IP telephones are located in different time zones than the host system. In these cases, the local time of day should be shown instead of the system time on the display of the digital telephones that are connected to the remote AP or on the display of the HFA IP telephones.

For a detailed description, refer to the section „Different Time Zones (DTZ)“.

2 Access Point Emergency Feature Description

2.1 Previous Survivability Function (HiPath 4000 V1.0)

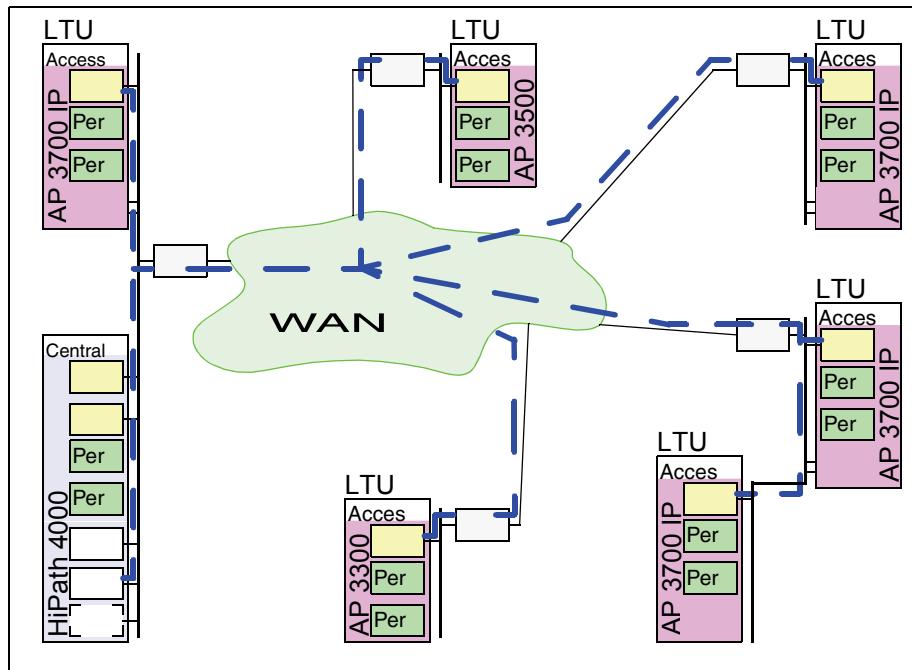


Figure 13 IPDA without survivability

In the basic configuration (without the survivability feature), an IPDA installation function depends completely on the availability and reliability of the LAN/WAN infrastructure used. The failure of an access point's IP connection leads to access point failure.

A total failure of the IP infrastructure results in the failure of all access points. Only the central system and the “classic” peripheral units connected continue to work.

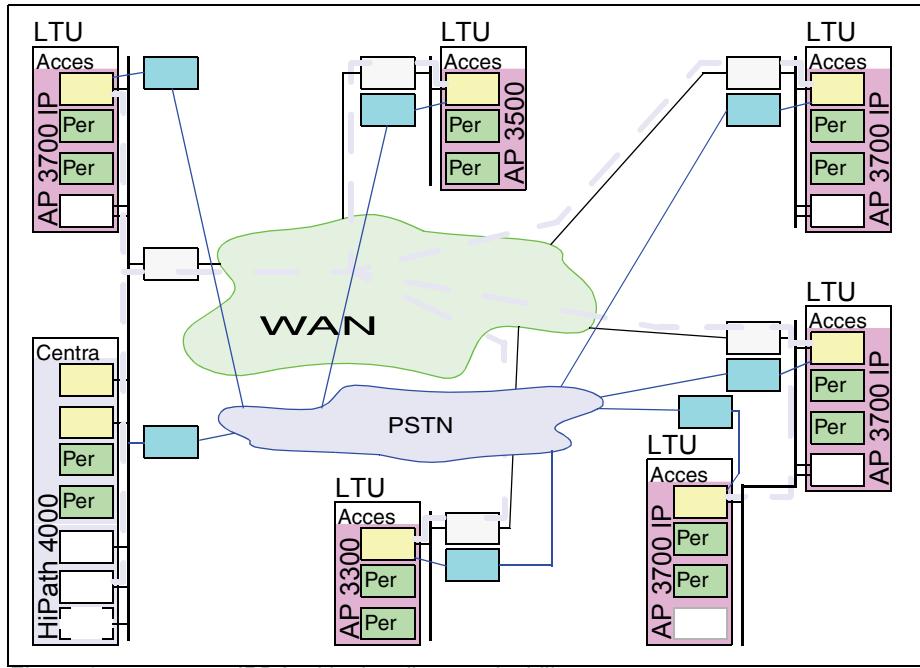


Figure 14 IPDA with signaling survivability

The signaling survivability feature uses alternative routes to maintain the signaling connection between the central system part and the access point.

If the LAN/WAN-based connection to the access point fails, a modem connection is established via CO. The access point is controlled via this connection until the LAN/WAN connection is reestablished.

If every access point features an individual modem (and the central system has reserved enough router connections via CO (PSTN)), signaling survivability can cover even the total failure of the WAN infrastructure. The only critical factor here are the connection between the active CC and the survivability router(s) in the HiPath 4000 LAN segment and the independence of (failed) WAN from the PSTN used for survivability.

The signaling path is switched over without interruption.

However, signaling survivability does not help against a central system failure. If a central system is no longer available to control the access points, a signaling path via CO is no help either. In such cases, the entire communication system (including all access points) fails.

2.2 Access Point Emergency Implementation Scenarios

The Access Point Emergency feature lets you operate access points in an emergency irrespective of whether or not the central system is available.

Access Point Emergency Feature Description

Access Point Emergency Implementation Scenarios

Options for operating access points from additional, physically separable control systems are provided for this purpose. These additional control systems (survivability units) can be mounted in each AP 3700 IP access point.

In principle, you can control all access points associated with a HiPath 4000 system from a single survivability unit (depending on the survivability unit's processor performance). Most of these scenarios avoid the use of "classic" shelves with a TDM connection and only use IPDA access points. The central control unit - the communication server - is often housed in the main computer center while the access point with the survivability unit is located in the standby computer center. The access points are distributed on the campus and networked over a high-availability IP infrastructure. If the communication server in the main computer center is not available, the survivability unit takes over the entire system operation.

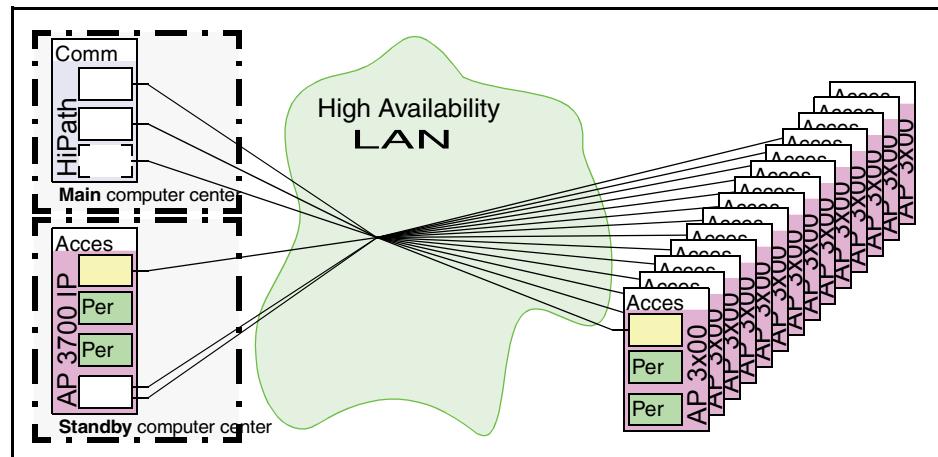


Figure 15 LAN scenario

The survivability unit is indicated by the abbreviation CC-AP in all figures and on all operational user interfaces. This is based on the logic used for naming control processor (CC-A, CC-B).

If the network features WAN routes that connect sites with several IPDA access points, for example, we recommend installing an individual survivability unit on each of these LAN islands. The access points can then be operated autonomously not only in the event of a central control unit failure but also if the WAN connection fails.

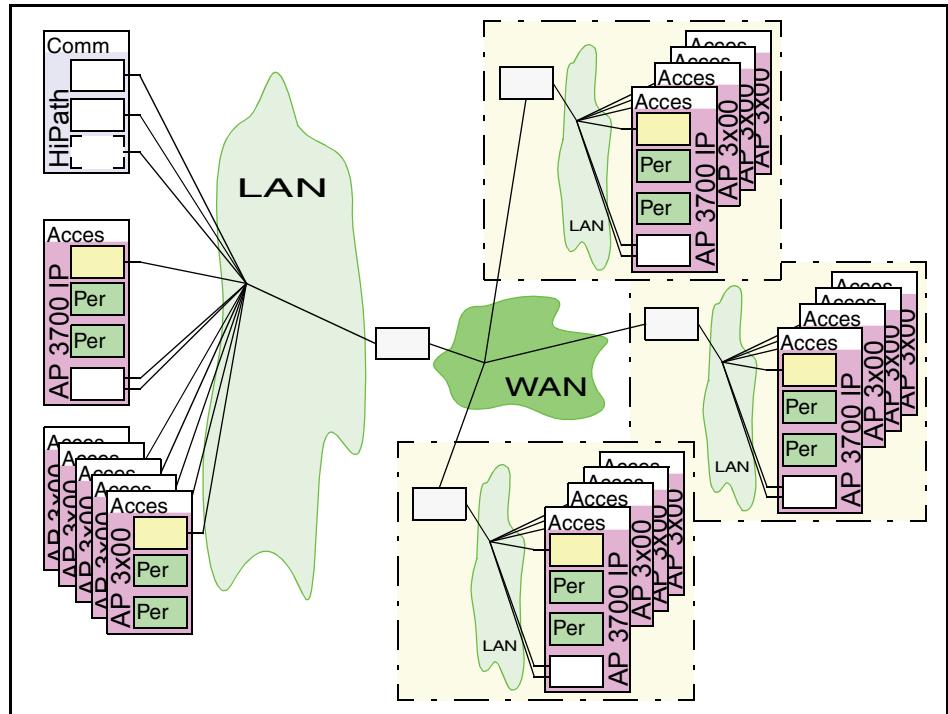


Figure 16 LAN/WAN scenario

In the classic branch structure, numerous relatively small but broadly distributed branches are connected via precisely dimensioned WAN routes to the company's central system. In this scenario, we recommend providing a survivability unit for the IPDA access point in each individual branch. In this way, you can ensure autonomous branch operation in the event of failure of the central control unit or WAN connection.

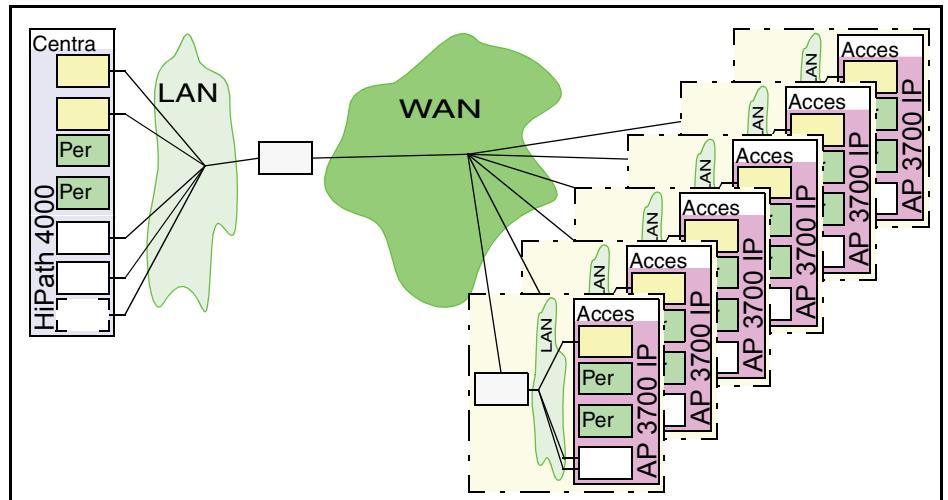


Figure 17 Branch (WAN) scenario

2.3 Access Point Emergency and Signaling Survivability

The new AP Emergency feature described here and the trusted signaling survivability feature introduced in HiPath 4000 V1.0 are not alternatives. Instead, they complement each other. A reliable layer concept for system stability can be implemented in all scenarios containing WAN routes.

1. Signaling survivability guarantees access point operation over the central control unit in the event of a WAN malfunction. The signaling survivability path is switched over without interruption.
2. AP Emergency takes over access point operation if the central control unit fails.

Figure 18 “AP Emergency scenario” illustrates a mixed scenario that will be referred to throughout the manual. In this figure, the broken blue lines represent the communication paths between the central control unit and the access point and the red dotted lines represent communication between the survivability units and the access points allocated to them.

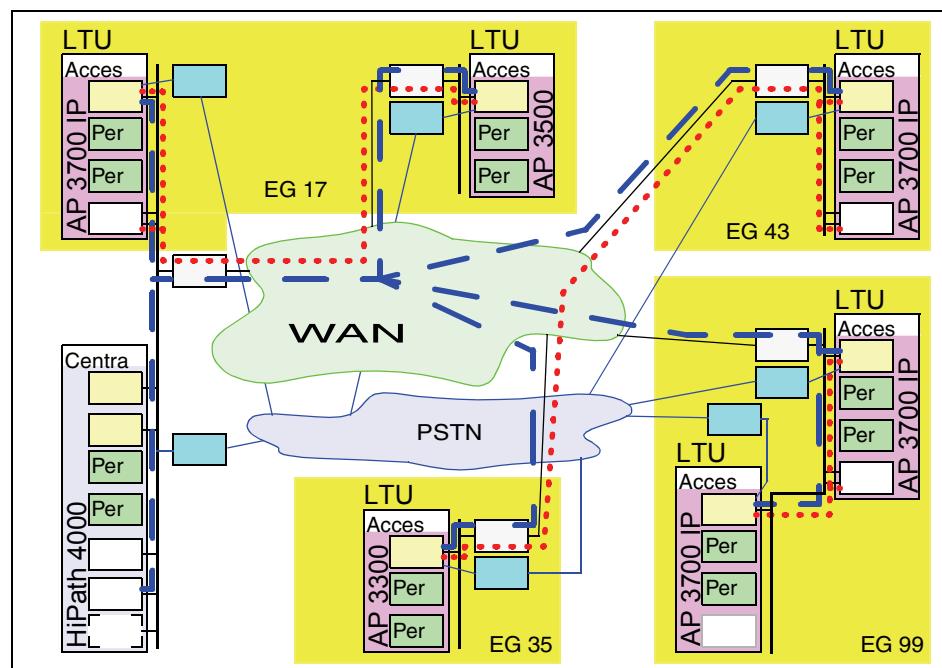
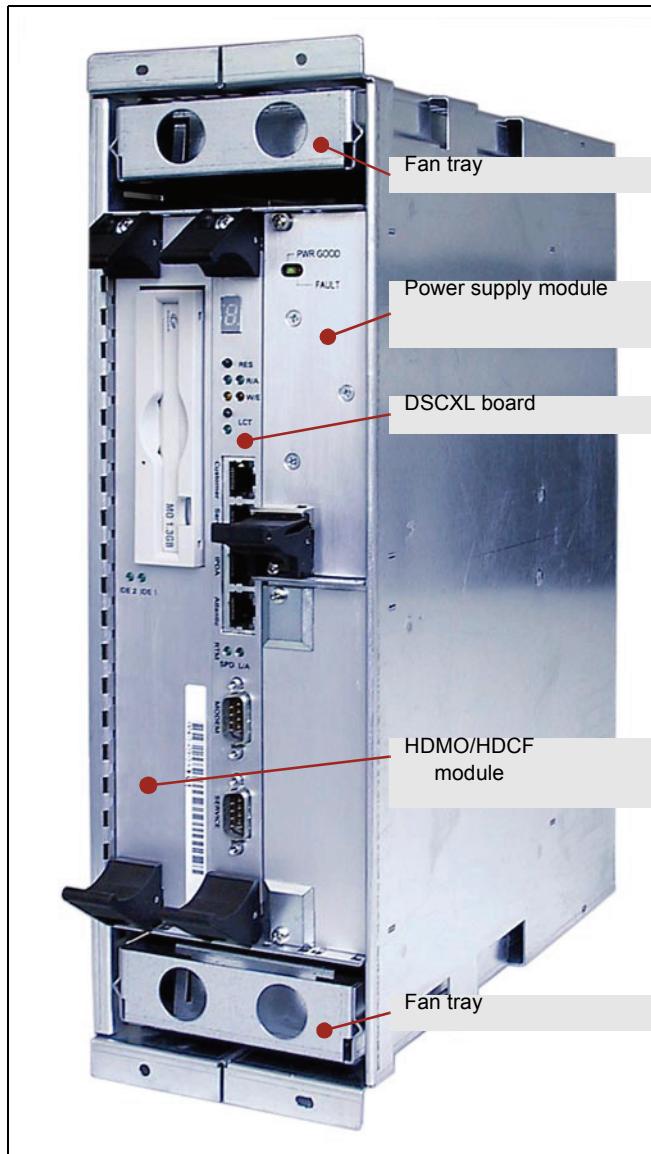


Figure 18 AP Emergency scenario

2.4 Survivability Unit



The survivability unit can only be used in AP 3700 IP access points. However, it can control all possible IPDA access point models (AP 3300 IP, AP 3500 IP, AP 3700 IP) in emergency mode. Access points are controlled regardless of whether the access point features NCUI2 or NCUI4.

The survivability unit consists of a cassette with cPCI backplane, DSCXL processor, HDMO module, power supply and redundant fan trays.

Depending on the power supply module, it can be powered with 110/230 V alternating current or 48 V direct current.

In AP 3700 IP, there is no electrical connection between the access point and the survivability unit.

Access Point Emergency Feature Description

Allocating Access Points to a Survivability Unit

Communication between the survivability unit and the NCUI2/4 on the same access point only runs via the IP network.

2.5 Allocating Access Points to a Survivability Unit

Access points are not directly allocated to a survivability unit. Instead, they are allocated to an emergency group. The group defines which access points are to be treated the same.

For example, it does not make sense to switch control of an individual access point without trunk access from the central system to a survivability unit. It makes more sense to switch an entire group in one go that also contains an access point with trunk access. Switchover regulations are defined per access point and group.

By introducing the abstract emergency groups, you can control several groups independently of a shared survivability unit.

The hierarchical assignment is simple:

- An access point can belong to exactly one emergency group.
- An emergency group can be controlled by exactly one survivability unit.

All combinations with 1 to 83 access points in 1 to 83 emergency groups on 1 to 83 survivability units are possible. However, you must calculate the necessary processor performance (the survivability unit corresponds to a monoprocessor system) to ensure that the survivability unit is not assigned any more access points than allowed by the processor performance. Because of that a maximum of 40 access points for each mono processor system or survivability unit is allowed.

There are two kinds of access points, depending on the type of connection; these are “Direct Link” (APDL) and “Networked” (APNW). For details, see [Section 4.2, “Configuring an Access Point”, on page 57](#).

NOTE: A survivability unit in an APNW access point **cannot** control any APDL access points.

However, a survivability unit in an APDL access point can control both APDL and APNW access points.

2.6 Switchover in Emergency Mode

When a HG 3575 discovers an interruption of the signaling connection to the central control unit, it reports this event to the allocated survivability unit.

Emergency mode, that is, when access point is controlled by a survivability unit, is the one escalation level higher than signaling survivability. If signaling survivability is configured when the connection is lost, signaling survivability first attempts to control the access points via modem. Emergency mode is initiated if this fails (for example, because central control unit is not available).

The survivability unit uses preconfigured rules to decide whether it should take over access point control or not.

- Each access point is assigned a weight.
- If the total weight of all access points in an emergency group that has lost its connection to the central control unit is greater than the limit specified, the survivability unit assumes control of all access points assigned to this group
- However, access points can also be configured so that they can always be individually controlled by the survivability unit regardless of their weighting.
- In addition, you can switch control of
 - individual access points
 - all access points in an emergency group
 - all access points in all emergency groups in a survivability unit or
 - all access points in the entire HiPath 4000 systemto the assigned survivability unit(s) at any time.

The survivability unit takes over control of the access point by instructing the HG 3575 to initiate a restart and then start up with the survivability unit. The HG 3575 restart triggers a restart in all peripheral boards on the access point.

- All calls are cleared down.
- Features with active logon, e.g. mobile subscribers (PIN, mobile HFA), are logged off.
- Features that can be configured by the user, such as key layout for (name keys, DSS keys), forwarding key, reminder key, etc., are set up in the state that they were in when the data was incorporated from the central system (see also [Section 2.8, “Configuration Data”](#)).

2.7 Reverting to Normal Operation

When a HG 3575 discovers that the signaling connection to the central control unit has been restored, it reports this event to the allocated survivability unit.

Access Point Emergency Feature Description

Configuration Data

The survivability unit uses preconfigured rules to decide whether or not it should hand back access point control to the central system.

- Every access point in an emergency group must have a stable connection to the central system for a minimum set time
- Automatic reversion is only permitted during a set interval during the day. The interval can be set to 24 hours so that automatic reversion is possible at any time.
- Automatic reversion can be deactivated.
- You can also switch back control of
 - individual access points
 - all access points in an emergency group
 - all access points in all emergency groups in a survivability unit or
 - all access points in the entire HiPath 4000 systemto the central control unit at any time.

The survivability unit returns access point control to the central control unit by instructing the HG 3575 to initiate a restart and then start up with the central control unit. The HG 3575 restart triggers a restart in all peripheral boards on the access point.

- All calls are cleared down.
- Features with active logon, e.g. mobile subscribers (PIN, mobile HFA), are logged off.
- Features that can be configured by the user, such as key layout (name keys, DSS keys), forwarding key, reminder key, etc., are set up in the state which is active in the central system - i.e. generally as it was prior to switchover.

2.8 Configuration Data

The entire HiPath 4000 system including all its access points and survivability units is only configured in the central system.

Local administration is not possible at the survivability unit (with the exception of UNIX, HiPath Backup Restore).

A special backup of the HiPath 4000 system database (HiPath backup restore in the central system) is performed at set intervals (usually once a day).

The survivability units perform continuous checks (every 10 minutes) to see if a new HiPath 4000 database backup is available. If this unit is not actively controlling an access point (emergency mode), it downloads the saved data and incorporates it by means of a reload (HiPath backup restore on the survivability unit).

The backup data is stored on a file server. This file server may be located in the customer's computer center. You can also use the HiPath 4000 Manager platform as a file server. This task can also be performed by the central system's ADP in exceptional circumstances.

The daily backup is configured on the file server in such a way that it always contains the complete system with database, patches, and software.

However, transmission from the central system to the file server and from the file server to the survivability unit is optimized. Only different data is actually transferred.

2.9 Transferring New System Releases and Patches

HiPath 4000 system complexity is considerably increased by survivability units. To keep operation and maintenance costs low, system releases and patches are automatically distributed to the survivability units.

In addition, new system releases and patches are incorporated in the backup/restore process for the database (see [Section 2.8, “Configuration Data”](#)).

2.10 Connection Between Subsystems (Islands)

If a HiPath 4000 system breaks down in emergency mode into several autonomous islands, how can the islands then communicate with each other? An autonomous island is defined as a survivability unit and all the access points over which the unit currently has active control.

Everything else remains the same within each individual island:

- Calls between subscribers in the same access point are switched within the access point.
- Calls between subscribers in different access points of an island are switched via IP connections between the access points.
- Incoming/outgoing trunk calls are conducted via the island's trunk interfaces.
- Incoming/outgoing calls in networked systems are conducted via the island's tie trunk interfaces.

What happens to calls for subscribers on another island?

Access Point Emergency Feature Description

Time Synchronization

All survivability units have the same complete central system database. Therefore, every island knows every subscriber in the entire configuration, including all subscribers on other islands. Access points outside the island are configured but cannot be reached. All boards and their subscribers, trunks and tie trunks are therefore known and belong to a set hierarchy (UNACH).

Although the IP infrastructure between some islands may still be intact, no inter-island calls between access points are switched via IP.

Trunk interfaces can still be used for inter-island communication. It is therefore still possible to reach a subscriber who is known but not directly available in another island over CO. The “Alternate Routing on Error” feature supports rule-based call number modification in emergency mode.

This feature guarantees Basic Call connectivity for traffic between the islands.

For this feature to work, the trunks on the islands must use different access codes. If all trunks use the same access code, directed routing must be performed by the carrier using the complete number dialed. (CENTREX).

If the islands are integrated in an extensive HiPath 4000 network with QSig trunks, the LCR configuration must include normal and emergency mode because the system has only one configuration. Even in this scenario, Basic Call connectivity is guaranteed for incoming, system-wide traffic to an AP which results in a transit connection. In order to support network-wide features, the islands should be configured as virtual nodes.

Payload survivability does not work in emergency mode as the islands involved no longer have a shared control unit.

2.11 Time Synchronization

An exact time is required for many HiPath 4000 functions (call detail recording, time-dependent channels, night service, etc.). Up until now there was only one clock per system, but with AP Emergency there are up to 84 clocks in the system and they have to operate synchronously.

There are two ways of synchronizing the time:

1. The IP network has a time server, which supports time synchronization of all HiPath 4000 processors (the central processor and all survivability units) using the Network Time Protocol.
2. A time server is **not** available in the IP network. The HiPath 4000 central system then makes its local time available over the network for synchronizing all survivability units.

2.12 Feature Licensing

A license is necessary for operating a survivability unit in a HiPath 4000 system.

All central system licenses are also used on the survivability units in emergency mode. The survivability units are operated without SIM cards. As a result, the 30-day grace period for license management begins as soon as the survivability unit starts actively controlling at least one access point. All features are disabled at the end of this 30-day period. However, if the 30-day license management grace period was already active on the central system and only 10 days of unrestricted operation remain (due, for example, to a defective SIM card) then this restriction also applies to all survivability units.

2.13 Application Support in Emergency Mode

The CAP (Common Application Platform) supports the AP Emergency feature so that a number of applications can function on both the central system and the survivability unit.

The prerequisites for this are:

- the application and CAP have a functioning IP connection to the survivability unit
- The application is based on CAP (CA4000 is not sufficient)
- the application only requires resources that are controlled by one and the same survivability unit.

Access Point Emergency Feature Description

Application Support in Emergency Mode

3 HiPath 4000 in the Customer LAN

In order to be able to control the IP-based access points, the HiPath 4000 control system must be given access to the IP network via which all access points can be reached. This is usually the customer's intranet. Once the "Atlantic LAN" is an internal HiPath 4000 network and may no longer be linked with the customer network, the control processors of the HiPath 4000 must receive additional LAN interfaces. Precisely which interfaces have to be retrofitted depends on the system architecture.

3.1 LAN Interfaces for the Processor Modules

NOTE: If UW7-based service applications such as the Quality of Service Viewer for IPDA are to be used or if access from the LCT on the access point to the central system is required, the LAN interface of the UW7 **must** be in the HiPath 4000 LAN segment (see [Section 4.1, "Configuring the HiPath 4000 LAN Segment", on page 38](#)).

Routing to the access points, which is configured for CC-A or CC-B, must also be configured in the UW7 in this case.

3.1.1 HiPath 4000 with DPC5 Processors

The monoprocessor architecture has a central processor on which not only the system control processes, but also administration and service software run under UNIX. The processor module is equipped with an external SL100 type LAN connection, in order for the UNIX software to access the customer network. If IP-based access points are to be controlled, an additional external LAN access link is required. To this end, the SL100 has to be replaced with the SL200 submodule.

In general, both LAN interfaces of the processor module are linked with the customer network on the SL200.

If separate processors are envisaged for CC and ADP, they each require a dedicated SL200. If the CC is of duplex design, both CCs also require an SL200. In this case only 1 SL200 Ethernet connection is actually required. An existing SL100 can continue to be used.

HiPath 4000 in the Customer LAN

Connecting the Local Craft Terminal (LCT) at the Access Point

3.1.2 HiPath 4000 with DSCXL Processors

The LAN connection for IPDA is located directly on the front panel in DSCXL processors. This connection must not be used if the processor works as an ADP in a duplex configuration.

3.2 Connecting the Local Craft Terminal (LCT) at the Access Point

Access points can be distributed from the central system components via IP. A typical location for a distributed access point is a branch office incorporated in the customer Intranet via IP.

If a new subscriber, for example, is now to be configured, the telephone is installed in the branch office. However, access to the computer in the central office is required for administration of the subscriber data. For this purpose, the LCT can be connected at the access point, in order to administrate the (entire) system from the access point.

If this is planned, an IP address is required not only for the access point, but also for the LCT connection. This address must also be agreed on with the network administration of the customer.

The LCT does not access the processors of the control system (CC-A/CC-B), but instead the UW7. If LCT access is supported by the access point, the LAN connection for the UW7 must be in the HiPath 4000 LAN segment. Routing to the access points, which is configured for CC-A or CC-B, must also be configured in the UW7 in this case.

The connection between LCT on the access point and the UW7 is only established via the LAN connection of the HG 3575 and not via the modem link in the case of signaling survivability. The restricted bandwidth of the modem connection would therefore not be sufficient.

A configuration example for the LCT can be found in [Chapter 9, “LCT configuration”](#).

NOTE: Before starting a PPP connection from the LCT on the access point to the central system, any existing terminal logon on the command line interface must be terminated. [logout].

3.3 Checking the IP Addresses Used

If all addresses required by the HiPath 4000 IPDA system have been agreed on with the network administrator of the customer, configuration can commence.

In order to rule out typos and mistakes, all IP addresses should be checked.

This is easily realized with HiPath 4000 Assistant. However, in order to do so, the LAN connection for the UW7 must be in the HiPath 4000 LAN segment.

Therefore, it is expressly recommended that configuration of the HiPath 4000 IPDA not be commenced until the UW7 is installed correctly and has access to the HiPath 4000 LAN segment.

It is thus possible to check the availability of any IP addresses from UNIX via the operating system command **ping**.

In other words, check that a new IP address can actually be reached prior to configuration via the **ping** command. If a response is received, the address already exists in the network.

If you wish to configure a CC-A address first, and the **ping** responds, you will have to obtain a different address from the network administrator, as an IP address may never be assigned twice. If, on the other hand, you wish to check the IP address of a router and receive no response, it will not be possible to link HiPath 4000 IPDA components via this router without taking additional measures.

HiPath 4000 in the Customer LAN

AP 3700 IP with Survivability Unit in the Customer LAN

3.4 AP 3700 IP with Survivability Unit in the Customer LAN

An AP 3700 IP with a survivability unit requires three connections in the customer's network:

1. HG 3575 LAN connection
2. DSCXL IPDA LAN connection
3. DSCXL CUSTOMER LAN connection

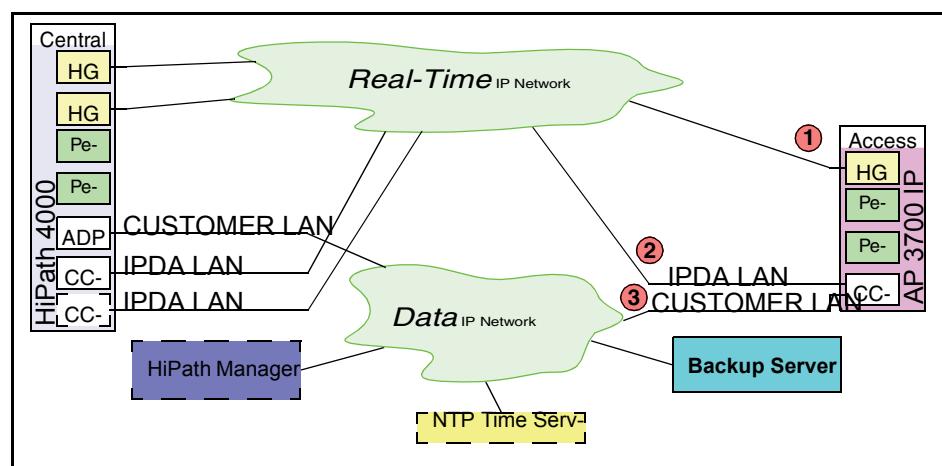


Figure 19 LAN interfaces of AP 3700 IP

The connections **1** (HG 3575) and **2** (IPDA/DSCXL) must be contained in the same LAN segment, as they must communicate with each other without an intermediary router.

Connection **3** (CUSTOMER-LAN/DSCXL) is required from the UNIX system of the survivability unit. The following functions are relayed via this interface:

HiPath Backup Restore - provision of current backup data from the backup server

- Error and alarm messages to HiPath Manager/Fault Management and System Management
- Access for applications such as Hardware Data Symptom Diagnosis, etc.
- Remote access for the service
- Collection of charge data collated on the survivability unit (COL)
- Synchronization of the system time with NTP time server or the HiPath 4000 central system

The interfaces **2** and **3** are deliberately listed separately. Many customers want a strict separation of their IP networks for data and voice. Connection **2** must be located in the voice NET for this type of scenario in order to communicate with the HG 3575. This also applies for connection **1**. Connection **3** can be located in the

data network. Here are no real-time requirements placed on the network. A consolidation could have prevented interface-related prioritization and reduced availability.

The requirements specified in [Section 3.3, “Network Requirements”](#) and [Section 3.4, “Network Data”](#) in document “HiPath Gateways HG 3500 and HG 3575”f or “IPDA” LAN ports also apply to interfaces **1** and **2**.

The capacity of interface **3** must be configured so that a system version can be completely restored from the backup server.

Assuming that one backup is performed daily and that all survivability units can restore simultaneously and without restrictions, a minimum bit rate of 24 Kbps is required. The maximum possible amount of data (all data is modified and must be transferred) is then transferred in ten hours.

The backup server must have enough memory for a complete backup set. This requires a maximum of approx. 100 MB.

HiPath 4000 in the Customer LAN

AP 3700 IP with Survivability Unit in the Customer LAN

4 Configuring the IPDA Feature

HiPath 4000 IP distributed architecture is rather a platform expansion than a typical new feature. Therefore, the configuration of this feature is broken down in the following section into typical steps, which are to be performed in consecutive sequence:

- Configuration: HiPath 4000 LAN segment - [Section 4.1 on page 4-38](#)
- Configuration: Access Point (*networked or direct link*) - [Section 4.2 on page 4-57](#)
- Configuration: HG 3500 as HG 3570 - [Section 4.3 on page 4-96](#)
- Configuration: Subscriber, trunk and tie trunk connections in access points - [Section 4.9 on page 4-168](#)

If necessary, the following steps are performed subsequently:

- Configuration: Special routes - [Section 4.4 on page 4-101](#)
- Configuration: Signaling survivability - [Section 4.5 on page 4-112](#)
- Configuration: Quality monitoring for the signaling connection over IP - [Section 4.6 on page 4-132](#)
- Configuration: Source dependent routing - [Section 4.7 on page 4-145](#)
- Configuration: Payload survivability - [Section 4.8 on page 4-149](#)

The corresponding sections contain configuration examples and detailed explanations of all requisite AMOs and AMO parameters. A distinction is made between



configuration with Configuration Manager and

configuration with AMO.

Information on CMI can be found in [Section 4.11, “Information on CMI”, on page 181](#).

The notes in [Section 4.12, “IP Address Changes”, on page 182](#) must be observed if the IP addresses in the HiPath 4000 LAN segment are to be changed in an active system (for example, because the network carrier changes the network address).

The creation of the “Access point Emergency“ feature is described in [Chapter 5, “Configuring the APE Feature \(Access Point Emergency\)“](#).

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

4.1 Configuring the HiPath 4000 LAN Segment

The HiPath 4000 LAN segment is that part of the customer network in which the IP components of the central system and direct link (i.e. not via router) access points are installed.

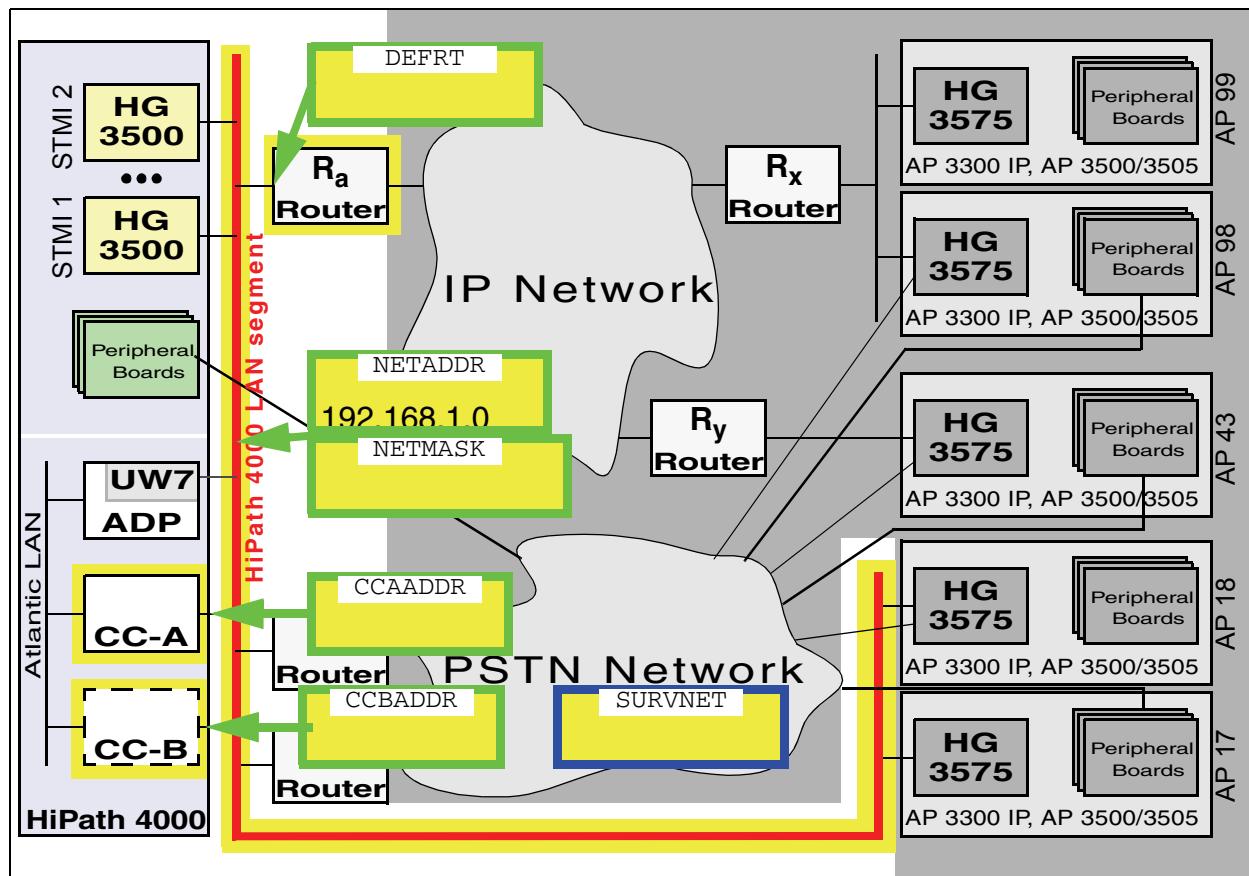


Figure 20 HiPath 4000 LAN segment

| | | |
|------------|----------------------|------------------------|
| ADD-SIPCO: | NETADDR=192.168.1.0, | NETMASK=255.255.255.0, |
| | DEFRT=192.168.1.254, | CCAADDR=192.168.1.1, |
| | CCBADDR=192.168.1.2, | SURVNET=192.168.15.0; |

At maximum capacity, a configuration requires a considerable number of IP addresses in this network, namely

- CC-A, CC-B, ADP: 3
- HG 3500: Up to 83
- Directly linked HG 3575: Up to 83
- TAP at a directly linked HG 3575: Up to 83
- Survability routers: Up to 10

Therefore, it is advisable to configure a dedicated LAN segment for the central part of a large HiPath 4000 installation and not permit any more nodes within that segment (particularly file servers, etc.)

For demo installations in which the HiPath 4000 LAN segment remains isolated, IP addresses from the private address range pursuant to RFC 1597 can be used. These do not require international coordination. For example, the range from 192.168.1.1 to 192.168.1.255 with netmask 255.255.255.0 can be recommended as the Class C address range.

Generation

Addresses (LSNET)

The first step in configuring IP distributed architecture involves the configuration of the HiPath 4000 LAN segment.

Configuration:



Configuration Management --> System Data --> IPDA --> IPDA System Data
Click **Search**, enter the required IP addresses and **Save**.

**ADD-SIPCO:NETADDR=192.168.1.0,NETMASK=255.255.255.0,
DEFRT=192.168.1.254, CCAADDR=192.168.1.1,
CCBADDR=192.168.1.2,SURVNET=192.168.15.0;**

If an isolated configuration is to be set up, the default router must be configured with the zero address 0 . 0 . 0 . 0 . In this case, only “direct link” access points can be configured (see [Section 4.2.2, “Configuring a “Direct Link” Access Point”, on page 68](#)). In [Figure 20 “HiPath 4000 LAN segment”](#), Router R_a is the default router.

If there is no second processor, the CCBADDR parameter need not be specified.

The SURVNET parameter can be dispensed with if signaling survivability is not required. If, however, the customer has purchased signaling survivability, i.e. if the corresponding license counter is greater than zero, then a survivability network address (see [Section 4.5, “Configuring Signaling Survivability”, on page 112](#)) must be specified. This can also be achieved with a dummy entry (zero address 0 . 0 . 0 . 0), though the signaling survivability function is not available in this case.

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

| | |
|---|--|
| <p>DPC5 processor: The lower LAN connection marked LINK2 on the SL200 board is used for IPDA.</p> <p>DSCXL processor: The LAN connection marked IPDA on the DSCXL is used.</p> | |
|---|--|

The licenses for signaling survivability can be queried as follows:



Configuration Management --> HiPath Inventory Management
--> HIM System Data --> Feature --> Marketing Units
Click **Search** --> **Sales Features tab** --> **Signaling Survivability entry**



DISP-CODEW; “**SIGNALING SURVIVABILITY**” entry

The values specified with ADD-SIPCO are immediately valid.

The LAN address of the UW7 operating system must be taken into account in the UW7 configuration. This configuration should already be completed prior to configuring the HiPath 4000 IPDA components.

NOTE: If access is requested from a TAP connected to the Access Point to the PBX, the UW7 LAN interface **must** be located in the HiPath 4000 LAN segment. Routing to the access points (which will be configured for CC-A or CC-B) also needs to be configured in UW7.

NOTE: Prior to ADD-SIPCO, use **ping** to check that the IP addresses given to you by the administrator are reachable.

CCAADDR and **CCBADDR** must not be reachable as this would indicate that the corresponding address had already been assigned.

DEFRT must be reachable (if not 0.0.0.0).

NOTE: Following ADD-SIPCO the active processor must be reachable in its network segment.

The standby processor in duplex systems does not respond (as long as it is in standby mode). Since routes have not yet been configured, the active processor cannot answer ping requests from other network segments!

Change:

All parameters configured here can be changed later.



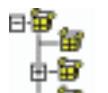
Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, change the addresses and **Save**.



CHANGE-SIPCO:TYPE=LSNET;

The parameters are not immediately effective after the CHANGE, but only once the system has been restarted. The database must be backed up beforehand to disk.



The restart can only be performed in expert mode.

Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO

(see AMO command)



EXEC-UPDAT:BP,ALL;

EXEC-REST:SYSTEM,RESTART;

NOTE: Changing the IP address has multifarious effects on a running system. If changes are necessary, a strict change sequence must be complied with, or else the access points will be irrevocably disconnected.

In this context, see [Section 4.12, “IP Address Changes”, on page 182](#).

Delete:

If, for instance, HiPath IPDA is to be completely removed from the system after a test, all access points and HG 3500, as well as the SIPCO configuration, also have to be deleted after the uninstall routine is completed. The links/LAN modules for the HiPath 4000 LAN segment can then also be removed. You must restart the system.



Deletion can only be performed in expert mode.

Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO

(see AMO command)



DELETE-SIPCO;

EXEC-UPDAT:BP,ALL;

EXEC-REST:SYSTEM,RESTART;

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

List of AMO parameters for Add / Change:

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|--|
| SIPCO | NETADR | d | Netzadresse des HiPath 4000 LAN Segments gilt für CC-A, CC-B, alle HG 3500 (STM12/4), Default-Router, Survivability-Router und direkt angeschlossene Access Points |
| | NETADDR | e | Network Address of the HiPath 4000 LAN Segment valid for CC-A, CC-B, every HG 3500 (STM12/4), default router, survivability router and directly linked Access Points |
| | NETMASK | d | Netzmaske des HiPath 4000 LAN Segments gültig wie NETADR |
| | NETMASK | e | Netmask of the HiPath 4000 LAN Segment valid like NETADDR |
| | DEFRT | d | Default-Router im HiPath 4000 LAN Segment über diesen Router sollen alle nicht direkt im HiPath 4000 LAN Segment angeschlossenen Access Points von den HG 3500 Baugruppen erreicht werden. Angegeben wird die IP-Adresse der Routers im HiPath 4000 LAN Segment. Falls kein Default-Router benutzt werden soll, z. B. für isolierte Demo-Installationen mit "direct link" APs, muss die Adresse 0.0.0.0 angegeben werden. |
| | DEFRT | e | Default Router in the HiPath 4000 LAN Segment via this router all Access Points that are not directly linked to the HiPath 4000 LAN Segment shall be reached by all HG 3500 boards.. The IP address of this router in the HiPath 4000 LAN Segment is to be given. If no default router shall be used, e.g. for stand-alone demo installations with "direct link" APs, give the address 0.0.0.0. |
| | CCAADDR | d | IP-Adresse des CC-A Prozessors im HiPath 4000 LAN Segment |
| | CCAADDR | e | IP address of the CC-A Processor in the HiPath 4000 LAN Segment |
| | CCBADDR | d | IP-Adresse des CC-B Prozessors im HiPath 4000 LAN Segment Nicht angeben, wenn kein CC-B im System |
| | CCBADDR | e | IP address of the CC-B Processor in the HiPath 4000 LAN Segment Omit, if no CC-B in the system |

Table 1

AMO SIPCO parameters in ADD branch or for CHANGE under
TYPE=LSNET

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|--|
| | SURVNET | d | Netzadresse des Survivability Netzes Die Netzmaske für das Survivability Netz ist mit 255.255.255.0 ebenso fest vorgegeben wie die Adressierung der einzelnen Knoten. Die Survivability-Router 1..10 haben die Adressen 1..10, die Access Points 17..99 die Adressen 17..99 im letzten Byte. Die vorgegebene Netzmaske schränkt die Klasse (A,B oder C) der Netzadresse nicht ein. Das Survivability Netz kann ein Subnetz eines Klasse A Netzes mit Netzmaske 255.255.255.0 sein. |
| | SURVNET | e | Network Address of the Survivability Network The netmask for the Survivability Network is fixed to 255.255.255.0 as well as the individual node addresses. The survivability routers 1..10 are addressed 1..10, Access Points 17..99 have address 17..99 in the last byte. The given netmask does not limitate the class (A,B or C) of the network address. The Survivability Network can be a subnet of a class A network with netmask 255.255.255.0. |

Table 1 AMO SIPCO parameters in ADD branch or for CHANGE under TYPE=LSNET

Quality of Service Parameters (DIFFSERV)

The following parameters can be set:

- For the physical Ethernet interface of CC-A and CC-B [BITRATE]
- For QoS support on Layer 2 to IEEE 802.1 q/q [VLAN, VLANID]
- For QoS support on Layer 3 to IETF RFC 2474 (DiffServ)
[TOSSUPV, TOSPL, TOSSIGNAL, TOSRTO]
- the lowest port used for payload connections (UDP/RTP+RTCP)

The Ethernet interface setting **must** be **identical** for all connected interface partners (CC-A and CC-B or LAN switches, routers).

NOTE: The setting of a fixed interface partner leads to problems with the “Autonegotiate” setting of the other partner.

Caution: Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply.

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

If the LAN ports with which CC-A and CC-B are connected do not support autonegotiation, or if autonegotiation does not function reliably, the Ethernet interfaces of the central processors can be set to fixed values.

VLAN tagging should only be activated when all routers in the network segment of the access point support VLAN tagging. The same applies for the DiffServ CodePoints. If the routers do not support DiffServ, the standard TOS values must be configured without DiffServ. If DiffServ is supported, but not the Siemens CodePoints, the values specified by the network carrier must be configured.

Given that some network component vendors only support prioritization with VLAN ID > 0 pursuant to IEEE 802.1 p/q, the VLAN ID can also be set. The HiPath HG 3575 module generally sets the priority bits when the VLAN option is activated. For values, see Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. According to the standard, the VLAN ID must then be set to zero, which also happens for the default setting.

The parameters for configuring the TOS bytes for the various traffic types are provisioned with the DiffServ CodePoints pursuant to the Siemens QoS Recommendation. VLAN tagging pursuant to IEEE 802.1 p/q is deactivated (VLAN=NO).

Example: Fixed setting to 100 Mbps full duplex



Configuration Management --> System Data --> IPDA --> IPDA System Data
Click **Search**, deactivate the **Enable Autonegotiation** checkbox under **Type of Service** on the **System Data** tab, enter **Speed** and **Mode** and **Save**.



CHANGE-SIPCO:TYPE=DIFFSERV,BITRATE=100MBFD;

The setting becomes effective on both CC-A and CC-B once the HiPath 4000 system is restarted. The database must be backed up beforehand to disk.



The restart can only be performed in expert mode.
Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO
(see AMO command)



EXEC-UPDAT:BP,ALL;
EXEC-REST:SYSTEM,RESTART;

If VLAN tagging pursuant to IEEE 802.1 p/q is supported in the HiPath 4000 LAN segment, it can be activated as follows:



Configuration Management --> System Data --> IPDA --> IPDA System Data
Click **Search**, activate the **VLAN Tagging** checkbox under **Type of Service** on the **System Data** tab, then **Save**.



CHANGE-SIPCO:TYPE=DIFFSERV,VLAN=YES;

If DiffServ is not supported, the TOS bytes must be configured with content pursuant to RFC 791 (see Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”).



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, enter the TOS values under **Type of Service** on the **System Data** tab, then **Save**.



CHANGE-SIPCO:TYPE=DIFFSERV,TOSPL=16,TOSSIGNAL=20;



Configuration Management --> Network --> System

Click **Save** on the Action pull-down menu.

The restart can only be performed in expert mode.

**Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO
(see AMO command)**



EXEC-UPDAT:BP,ALL;

EXEC-REST:SYSTEM,RESTART;

Note:

VLAN tagging changes the packet header. Many L2 switches or routers understand either packets with or without tagging. In other words,

- the relevant switches/routers also have to be adjusted.
- while the settings do not correspond, it is possible that packets will not be transmitted.
 - the conversion of the HiPath HG 3500 system interrupts payload connections
 - the conversion of the HiPath 4000 CCs interrupts the contact to all access points

A change of TOSPL is directly loaded on all HG 3500s and becomes effective immediately, without the operation of the modules having to be interrupted.

The parameter TOSSIGNAL does not become effective until the connection for which the TOS value is set has been cleared down and then set up again.

The disconnection and re-establishment of the links between the HiPath 4000 central system and access point can be realized through

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

- a soft restart on the HiPath 4000 system, which then affects all subscribers



The soft restart can only be performed in expert mode.
Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access -->
Open ...<IP> with AMO (see AMO command)



EXEC-REST:UNIT, BP, SOFT;

- through DEACTIVATE-USSU and ACTIVATE-USSU for every individual access point, which then only affects the respective subscribers.



Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **SEARCH** and select the access point.
Click **Deactivate** on the Action pull-down menu.
Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.



DEACTIVATE-USSU:LTU=xx;
ACTIVATE-USSU:UNIT=LTG, LTU=xx;

The TOS bytes at the access points are configured specifically for every access point.

If you want to locate the payload connections in a customer network in a specific port range for reasons of port-based prioritization, for example, then this can be set as follows:



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, enter the base address of the UDP port under **Type of Service** on the **System Data** tab, then **Save**.



CHANGE-SIPCO:TYPE=DIFFSERV, UDPPORT=40000;

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|--|
| SIPCO | TOSPL | d | TOS-Byte für die VoIP Payload-Verbindungen zwischen HiPath 4000 und Access Point. Gültig für Pakete von beliebigen HiPath HG 3500 in Richtung Access Point. |
| | TOSPL | e | TOS Byte for the VoIP payload connections between HiPath 4000 and Access Point. Valid for packets from any HiPath HG 3500 towards Access Point. |

Table 2

AMO SIPCO parameters in CHANGE branch under
TYPE=DIFFSERV

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|--|
| | TOSSIGNAL | d | TOS-Byte für die Signalisierungsverbindungen zwischen HiPath 4000 und Access Point. (<i>auch für Supervisory und RTO</i>) Gültig für Pakete vom CC-A, CC-B in Richtung Access Point. |
| | TOSSIGNAL | e | TOS Byte for the Signaling connections between HiPath 4000 and Access Point. (<i>also for Supervisory and RTO</i>) Valid for packets from CC-A, CC-B towards Access Point. |
| | VLAN | d | Schaltet VLAN-Tagging nach IEE 802.1p/q ein (JA) bzw. aus (NEIN). Gültig für VoIP Payload-Verbindungen von beliebigen HiPath HG 3500 in Richtung Access Point. Gültig für Pakete vom CC-A, CC-B in Richtung Access Point. |
| | VLAN | e | Switches VLAN Tagging according to IEEE 802.1p/q on (YES) or off (NO). Valid for VoIP payload connections from any HiPath HG 3500 towards Access Point. Valid for packets from CC-A, CC-B towards Access Point. |
| | VLANID | d | VLAN-ID Wert für alle HG 3500 sowie CC-A und CC-B Nur von Bedeutung, wenn VLAN=JA. 12 Bit Wert, der gemäß IEEE 802.1 p/q Standard auf Null gesetzt sein muss, wenn Priorisierung verwendet wird (VLAN=JA). Von dieser Standardeinstellung darf nur abgewichen werden, wenn Netzwerkkomponenten bestimmter Hersteller erzwingen, dass bei Nutzung der Priorisierung eine VLAN-ID > 0 zu verwenden ist. |
| | VLANID | e | VLAN-ID value for all HG 3500, CC-A and CC-B Only relevant if VLAN=YES. 12 Bit value that, according to IEEE 802.1 p/q, has to be set to zero when prioritization is used (VLAN=YES). This standard setting may only be changed, if network components of certain vendors enforce the usage of VLAN-ID > 0 while using prioritization. |
| | BITRATE | d | Einstellung der Ethernet-Schnittstelle von CC-A und CC-B bezüglich Bitrate und Betriebsmodus Die Einstellung beider Schnittstellenpartner (HG 3575 und Port am LAN-Switch, -Router) muss identisch sein! |

Table 2

*AMO SIPCO parameters in CHANGE branch under
TYPE=DIFFSERV*

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | BITRATE | e | Setting of Bitrate and Mode of Operation for the Ethernet Interface of CC-A and CC-B Both interface partners (HG 3575 and port of LAN-Switch or -Router) must be set identically! |
| | UDPPORT | d | Einstellung des Basis-Ports (niedrigste Portnummer) für Payloadverbindungen im IPDA-System Für jede Payload-Verbindung werden an den beteiligten Gateways HG 3500 bzw. HG 3575 ein UDP Port für RTP und ein weiterer für RTCP benötigt. Die Portnummern werden in einem Bereich von [UDPPORT .. UDPPORT+247] vergeben. RTP belegt dabei immer eine gerade Nummer, RTCP die nächst höhere ungerade. Wertebereich: [4352 .. 65038], nur gerade Zahlen erlaubt. |
| | UDPPORT | e | Setting of the Base Port (lowest port number) for Payload Connections in the IPDA System For every payload connection one UDP port is required for RTP and another for RTCP. The port numbers are assigned in a range of [UDPPORT .. UDPPORT+247]. RTP always uses an even number, RTCP the next higher odd one. Value range: [4352 .. 65038], only even numbers allowed. |

Table 2

AMO SIPCO parameters in CHANGE branch under
TYPE=DIFFSERV

The parameters TOSSUPV and TOSRTO from version 1 are no longer required and as such have been omitted.

Additional parameters

With ADD-SIPCO, additional system parameters are also set to default values which can be changed by means of CHANGE-SIPCO. These parameters are broken down into 2 groups.

System timing (TIMING)

Under TYPE=TIMING, central values of the system timing can be set for the monitoring of IP links. If the values set here are exceeded, the system switches the communication between HiPath 4000 and access point to the “signaling survivability” modem link or the access point is temporarily put out of operation.

In order to render the changed values in the affected access points effective, they **all** have to be restarted with



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.

Click **Execute** on the Action pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



EXEC-USSU:MODE=UPDATAP,LTU=xx;

NOTE: Connections are cleared down without further warning.

Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk. Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with EXEC-USSU:UPDATAP, LTU number , UL.

If the PINGTIME parameter has been changed, **all** HiPath HG 3500s must also be restarted with



Configuration Management --> System Data --> Maintenance --> Board Maintenance

Click **Search** and select all **STM12** and **STM14**.

Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.



RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2316-X;
und

RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2316-X10;
und

RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2324-X500;
und

RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2316-X510;

NOTE: Existing links are disconnected.

NOTE: It is crucial that TIMING changes are really loaded at all access points and HG 3500s, as otherwise the system reaction to the timer sequences would be inconsistent!

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|--|
| SIPCO | PINGTIME | d | <p>Zeitdauer, während der nach einer schlechten VoIP Payload-Verbindung zwischen 2 HiPath HG 3500/HG 3575 die Verbindungsqualität getestet wird. Ist die Verbindungsqualität bei Beendigung einer Verbindung zwischen 2 HG 3500/75 als schlecht markiert, wird für die Zeitdauer PINGTIME die Verbindung getestet. Fällt während dieser Zeit die Prüfung gut aus, wird die Prüfung abgebrochen und die Verbindung zwischen den betroffenen HG 3500/75 sofort wieder auf gut gesetzt. Ist das Ergebnis schlecht, wird während der gesamten Zeit weiter geprüft und erst nach Ablauf der PINGTIME die Verbindung auf gut gesetzt wird. Weitere Informationen siehe Figure 41 Blocks the IP connection for payload due to „Bad Quality“ on page 4-150.</p> <p>Der Wert wird in [s], Sekunden angegeben.</p> <p>Es wird empfohlen, diesen Parameter vom Default-Wert 60 auf den Maximalwert 3600 zu verändern.</p> |
| | PINGTIME | e | <p>Time interval for testing the payload quality between 2 HiPath HG 3500/HG 3575 after a VoIP payload connection has been terminated with quality marked bad.</p> <p>If the payload quality for a connection between 2 HG 3500/75 marked as bad upon termination of the connection, the connection is going to be tested for the duration of PINGTIME. With positive test results during this time interval the test is stopped immediately and the connection is marked good again. With negative results the tests will be continued until PINGTIME expires. After that the connection will be marked good again. For further Information see Figure 41 Blocks the IP connection for payload due to „Bad Quality“ on page 4-150</p> <p>The value is entered in [s], seconds.</p> <p>It is recommended to change this parameter from the default value 60 to the maximum value of 3600.</p> |

Table 3

AMO SIPCO parameters in CHANGE branch under TYPE=TIMING

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | RESTIME | d | <p>Zeit zwischen einem Schnittstellenfehler aus dem "Keep Alive" der Signalisierungsverbindung und dem Rücksetzen des Access Points (Wartezeit bis AP-Restart).</p> <p>Wird ein Schnittstellenfehler des "Keep Alive" der Signalisierungsverbindung gemeldet, startet das Zeitintervall RESTIME.</p> <p>Nach dem Schnittstellenfehler können keine neuen Gespräche vom/zu den betroffenen AP aufgebaut werden; bestehende Verbindungen bleiben abhängig vom IP-Netzwerk bestehen, jedoch kann es zu Nullwegen (100% Paketloss) kommen.</p> <p>Nach Ablauf des Zeitintervalls wird der Access Point zurückgesetzt. Alle Payload-Verbindungen gehen verloren, es sind keine neuen Payload-Verbindungen möglich, bis es der HiPath 4000 Zentrale wieder gelingt, Kontakt zum Access Point herzustellen.</p> <p>Der Wert wird in [s], Sekunden angegeben.</p> |
| | RESTIME | e | <p>Time between an interface fault specified in the "Keep Alive" message from the signaling link and the access point reset.</p> <p>The RESTIME interval starts when an interface fault is reported in the "Keep Alive" message from the signaling link.</p> <p>New calls cannot be set up from/to the relevant AP following the interface fault; existing connections are maintained depending on the IP network, but null paths can occur (100% packet loss).</p> <p>The access point is reset when the time interval expires. All payload connections are lost and no payload connections are available until the HiPath 4000 central system succeeds in establishing contact with the access point.</p> <p>The value is specified in seconds [s].</p> |
| | SUPVTIME | d | <p>Maximale Zeitspanne, während der auf einer Überwachungsverbindung (Supervisory-Verbindung) gewartet wird.</p> <p>Nur bei aktivierter Signaling Survivability. Auf der Supervisory-Verbindung werden in sehr kurzen Intervallen "Keep Alive" Meldungen gesendet. Kommt für länger als SUPVTIME kein Paket an, wird der Weg über das IP-Netz als gestört betrachtet, die Modemverbindung zum Access Point aktiviert und dieser Weg für die Signalisierungsverbindung zwischen HiPath 4000 und Access Point verwendet.</p> <p>Der Wert wird in [s], Sekunden angegeben.</p> |

Table 3

AMO SIPCO parameters in CHANGE branch under TYPE=TIMING

Configuring the IPDA Feature
Configuring the HiPath 4000 LAN Segment

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|--------------|----------------------|--|
| | SUPVTIME | e | Maximum time waiting for a packet on the Supervisory connection Only if Signaling Survability is activated. On the Supervisory connection “keep alive” messages are sent in very short intervals. If SUPVTIME exceeds without a packet arrived, the way through the IP networks is considered as disturbed. The modem connection to the Access Point is activated. The signaling between HiPath 4000 and Access Point is routed via the modem connection. The value is entered in [s], seconds. |
| | APESWDL Y | d | APE Umschalteverzögerung <i>nur wirksam mit dem Leistungsmerkmal AP Emergency!</i> siehe Section 5.10, “Defining the Switchover Delay”, on page 205 Das Umschalten eines Access Points in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Es ist entweder Null - “schalte sofort“ einzutragen, oder die Zeit, welche von der HiPath 4000 Zentrale benötigt wird, um einen RELOAD durchzuführen. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99]. |
| | APESWDL Y | e | APE Switch Over Delay <i>only effective with the feature AP Emergency!</i> see Section 5.10, “Defining the Switchover Delay”, on page 205 The switch-over of an Access Point into Emergency Mode can be delayed for a configurable amount of time. It shall either be set to zero - “switch immediately“, or to the amount of time which the central HiPath 4000 system needs to perform a RELOAD. The value is entered in minutes. Range [0 .. 99]. |

Table 3

AMO SIPCO parameters in CHANGE branch under TYPE=TIMING

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | ALVTIME | d | <p>Maximale Zeitdauer für den "Keep Alive" Mechanismus der Signalisierungsverbindungen zwischen HiPath 4000 und den Access Points. Vergeht diese Zeit ohne Antwort, wird ein Schnittstellenfehler gemeldet und der Access Point wird aus der ATTENDANCE LIST genommen (F5308, LTUC OUT OF ATTENDANCE LIST). Der Wert wird in [s], Sekunden angegeben. Wertebereich [20 .. 90]</p> <p>Hinweis: Wenn Signaling Survability konfiguriert ist, muss dieser Parameter auf einen Wert eingestellt werden, der größer ist als die Maximalzeit für den kompletten Aufbau der Signalisierungsverbindung über Modem!</p> |
| | ALVTIME | e | <p>Maximum time interval for the "keep alive" mechanism of the signaling connections between HiPath 4000 and the Access Points.</p> <p>If there is no answer during this interval, an interface error will be reported and the access point is taken out of the ATTENDANCE LIST (F5308, LTUC OUT OF ATTENDANCE LIST).</p> <p>The value is entered in [s], seconds. Range [20 .. 90].</p> <p>Note: When Signaling Survability is configured, this parameter must be set to a value greater than the maximum duration of the complete setup of signaling connection via modem!</p> |

Table 3 AMO SIPCO parameters in CHANGE branch under TYPE=TIMING

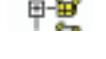
Payload Quality (PLQUAL)

Under TYPE=PLQUAL the limiting values for monitoring the payload quality, i.e. the voice links, are configured. If the upper limits are exceeded, additional voice links between the respective modules (HiPath HG 3500 and/or 3575) are established via the alternative route, provided one has been configured. If the lower limits are exceeded, the standard route is returned to the IP network.

The delay values only ever refer to one direction (A -> B or B -> A), and not to the "round-trip delay" (A -> B -> A). They are derived from the Real Time Transmission Control Protocol.



Configuration Management --> System Data --> IPDA --> IPDA System Data



Click **Search**, enter the limiting values under **Payload Quality** on the **System Data** tab and **Save**.



CHANGE-SIPCO:TYPE=PLQUAL, DLYHILIM=200, DLYLOLIM=120, LFRHILIM=3, LFRLOLIM=2;

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

The changed parameters are started on all access points and HG 3500s immediately and without interrupting operation.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| SIPCO | DLYHILIM | d | Obere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HiPath HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert wird in [ms], Millisekunden eingegeben. |
| | DLYHILIM | e | Upper delay limit for VoIP payload connections between HiPath HG 3500/HG 3575. When delay exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is entered in [ms], milliseconds. |
| | DLYLOLIM | d | Untere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HiPath HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert wird in [ms], Millisekunden eingegeben. |
| | DLYLOLIM | e | Lower delay limit for VoIP payload connections between HiPath HG 3500/HG 3575. When delay falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is entered in [ms], milliseconds. |

Table 4

AMO SIPCO parameters in CHANGE branch under TYPE=PLQUAL

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|--|
| | LFRHILIM | d | Obere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HiPath HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an. |
| | LFRHILIM | e | Upper limit for the fraction of lost packets on VoIP payload connections between 2 HiPath HG 3500/HG 3575. When the fraction of lost packets exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is the ratio of lost to sent packages in percent. |
| | LFRLOLIM | d | Untere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HiPath HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an. |
| | LFRLOLIM | e | Lower limit for the fraction of lost packets on VoIP payload connections between 2 HiPath HG 3500/HG 3575. When the fraction of lost packets falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is the ratio of lost to sent packages in percent. |

Table 4 AMO SIPCO parameters in CHANGE branch under TYPE=PLQUAL

Bandwidth table (BANDW)

Change the system-wide bandwidth table with AMO SIPCO, CHANGE branch under TYPE=BANDW.

Direct media connection (DMCDATA)

The parameter TYPE=DMCDATA specifies whether or not all HG 3500s support direct media connections. Only STMI2-type HG 3500 boards support DMC. DMC must be disabled if using STMI and STMI2 in mixed mode.

Configuring the IPDA Feature

Configuring the HiPath 4000 LAN Segment

In addition, the NWDMC parameter determines the codec type (G.711 or G.729) to be used for DMC connections in network scenarios with TDM subscribers. This information is provided for the Resource Manager only.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, enable or disable the **Direct Media Connection (DMC) activated** field on the **System Data** tab, select the code type, and **Save**.



CHANGE-SIPCO:TYPE=DMCDATA,DMCALLWD=N;NWDMC=G729;

The modified parameters are effective.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| SIPCO | DMCERL | d | Direct Media Connection erlaubt. Legt fest, ob Direct Media Connections auf allen HG 3500 zu unterstützen sind, oder nicht. |
| | DMCALLWD | e | Direct Media Connections allowed. Specifies whether Direct Media Connections are to be supported by all HG 3500 gateways - or not. |
| | NWDMC | d | Codec-Typ für DMC-Verbindungen in Netzwerk-Szenarien mit TDM-Teilnehmern. G711 oder G729 |
| | NWDMC | e | Codec Type for DMC connections in networking scenarios with TDM subscribers. G711 or G729 |

Table 5

AMO SIPCO parameters in CHANGE branch under
TYPE=DMCDATA

4.2 Configuring an Access Point

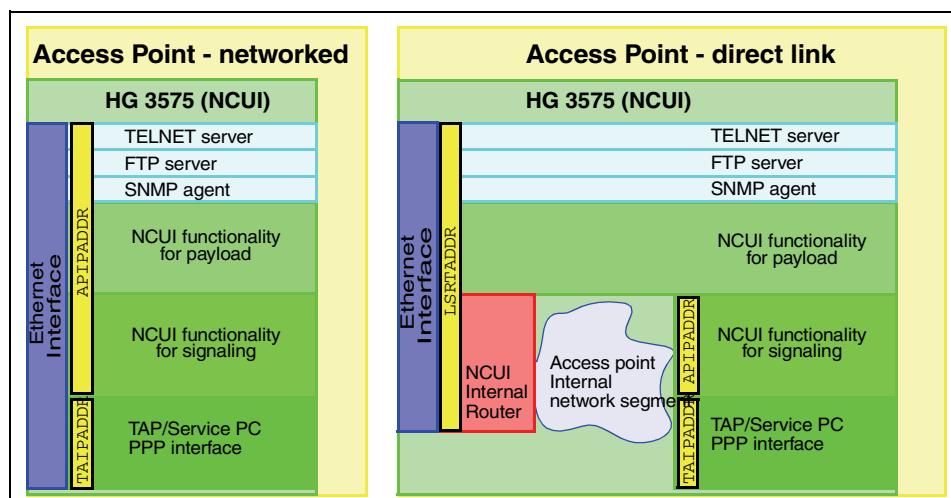
When configuring an access point, a distinction must be made as to

- whether the **access point involved is networked via routers in a network segment other than the HiPath 4000 LAN segment** (see [Section 4.2.1, “Configuring a “Networked“ Access Point”, on page 58](#)),

or

- whether the **access point is linked directly to the HiPath 4000 LAN segment** (see [Section 4.2.2, “Configuring a “Direct Link“ Access Point”, on page 68](#)).

[Figure 21 “Difference between “networked“ and “direct link“ access point”](#) illustrates the difference.



[Figure 21 Difference between “networked“ and “direct link“ access point](#)

In all cases, an access point need not only be configured in the system. In order to be able to address an access point, numerous data also has to be entered locally at the access point during its initial installation (see [Section 4.2.5, “Local Configuration of an Access Point”, on page 83](#)). System administration should always be performed first, followed by the local installation of the access point. The data to be entered at the access point can be derived by Configuration Management or directly from the data configured in the system using “HiPath 4000 Expert Access“.

Configuring the IPDA Feature

Configuring an Access Point

4.2.1 Configuring a “Networked“ Access Point

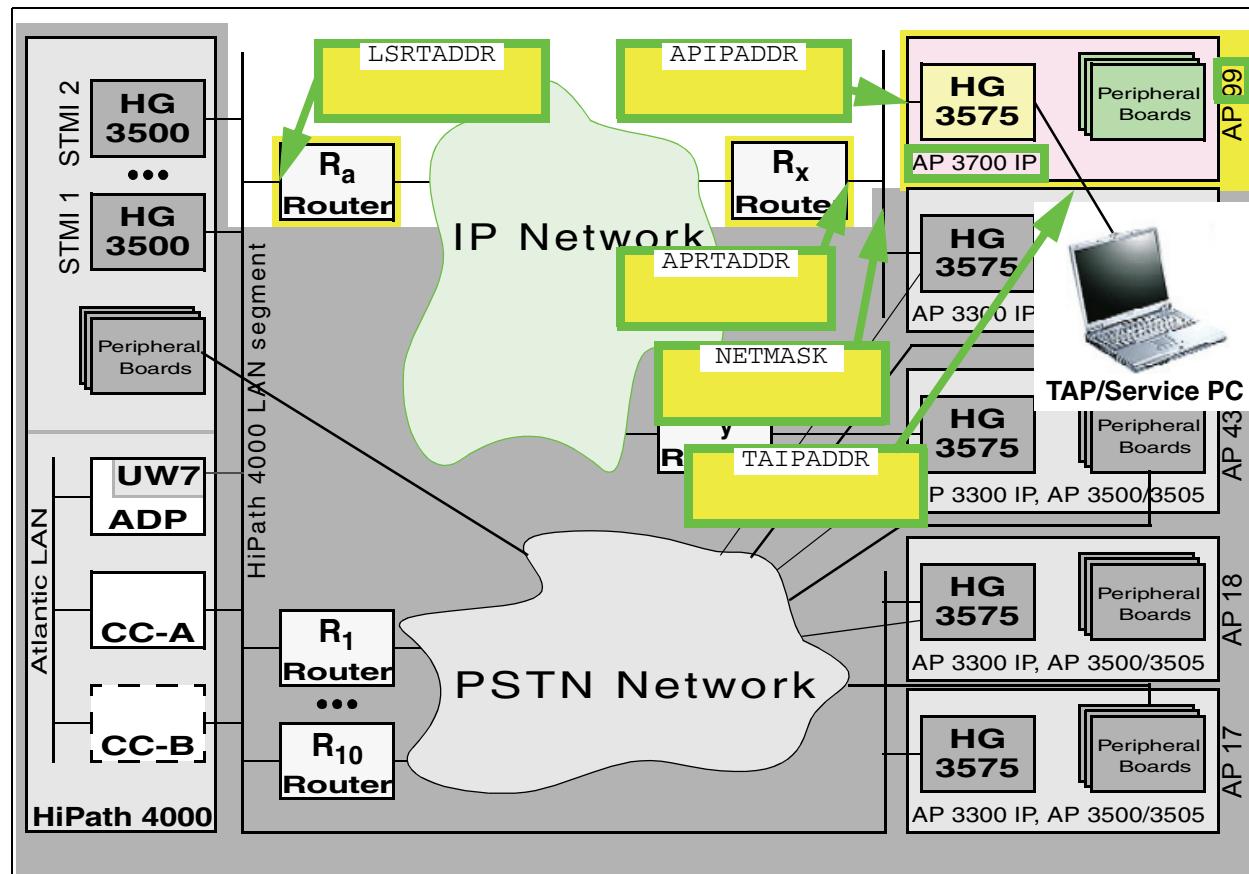


Figure 22 Configuring a “Networked“ access point

| | |
|--------------------------|----------------------------|
| ADD-UCSU: UNIT=AP, | LTU=99, |
| LTPARTNO=Q2305-X35 | SRCGRP=2, |
| FRMTYPE=AP 9837009, | CONNTYPE=APNW, |
| LSRTADDR=192.168.1.254, | APRTADDR=192.168.23.1, |
| LOCID=2, | LOCATION="BLN ROHRDAMM 85. |
| PHONE=03038612345, | GEB. 30-222", |
| PLCHECK=YES, | FAX=03038654321, |
| CONVLAW=NO; | BCHLCNT=40, |
| ADD-APRT: TYPE=APNET, | LTU=99, |
| APIPADDR=192.168.23.99, | NETMASK=255.255.255.0, |
| TAIPADDR=192.168.23.199; | |

Figure 22 “Configuring a “Networked” access point” shows the fundamental information required for configuring a “networked” access point

- The fact that the access point is linked via router with the HiPath 4000 LAN segment: Link type APNW, i.e. “networked”.
- The LTU number of the access point, i.e. 99.
- The LTU part number specifies the HG 3575 used.
- The access point’s shelf type is derived from the type designation.
- The IP address of the access point: 192.168.23.99.
- The IP address for the TAP/Service PC link at the access point: 192.168.23.199.
- The IP address of the router (port), via which AP99 accesses the HiPath 4000 LAN segment: 192.168.23.1.
- The netmask in the segment of the AP99: 255.255.255.0.
- The IP address of the router (port) at the HiPath 4000 LAN segment, via which the AP99 can be accessed by the central components in the HiPath 4000 LAN segment, i.e. in this case: 192.168.1.254.
- By limiting the number of B-channels, the bandwidth available to AP99 is indirectly reduced in the configuration example. This mechanism works independently of the bandwidth limitation performed by the Resource Manager in the “Large Enterprise Gatekeeper” Feature. For further information, please refer to [Chapter 6, “Load Calculation”](#).
- Should Payload Quality Handling be activated? For details see [Section 4.8, “Configuring Payload Survivability”, on page 149](#).
- The Source Group Index is explained in detail in [Section 4.7, “Configuring Source Dependent Routing”, on page 145](#).

Additional data is explained in more detail with the corresponding AMO parameters.

Generation

An access point is configured with three AMOs (UCSU, APRT, STMIB) and activated with USSU.

UCSU

With the AMO UCSU, the access point is configured as a new shelf in the system and its reachability via routers is ensured.

Configuring the IPDA Feature

Configuring an Access Point



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **New** and enter the LTU of the access point.

Enter the relevant data on the **General** and **IP Interface (NW)** (Connect Type=APNW) tab and **Save**.



```
ADD-UCSU:UNIT=AP,LTU=99,LTPARTNO=Q2305-X35,SRCGRP=2,  
FRMTYPE=AP37009,CONNTYPE=APNW,LSRTADDR=192.168.1.254,  
APRTADDR=192.168.23.1,LOCID=2,LOCATION="BLN ROHRDAMM  
85. GEB. 30-222",PHONE=03038612345,FAX=03038654321,  
PLCHECK=YES,BCHLCNT=40,CONVLAW=NO;
```

NOTE: The parameters FRMTYPE and CONNTYPE cannot be changed after the ADD!

NOTE: Prior to ADD-UCSU, use **ping** to check that the IP addresses given to you by the administrator are reachable.
LSRTADDR and APRTADDR must respond.

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|--|
| UCSU | LTSACHNR | d | Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/NCUI4. |
| | LTPARTNO | e | Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used. |
| | SRCGRP | d | Source Group Index Zuordnung des Access Points in eine Source Group für "Source Dependent Routing". (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben. |
| | SRCGRP | e | Source Group Index Assignment of the Access Point to a Source Group for "Source Dependent Routing". This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there. |

Table 6

APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

| AMO | Parameter | Sprache/ Language | Beschreibung/Description | |
|-----|-----------|----------------------|---|----------|
| | FRAMETYP | d | Typ des LTU-Rahmens (Shelf Typ) | |
| | | | AP-Typ | FRAMETYP |
| | | | AP 3300 IP | L80XF |
| | | | AP 3500 IP | INCH19 |
| | | | AP 3700 IP | AP37009 |
| | FRMTYPE | e | Type of the LTU Frame (Shelf Type) | |
| | | | AP-Type | FRMTYPE |
| | | | AP 3300 IP | L80XF |
| | | | AP 3500 IP | INCH19 |
| | | | AP 3700 IP | AP37009 |
| | VERBART | d | Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APNW - Access Point via Network: Access Point und Zentrale werden in unterschiedlichen IP-Netzen betrieben, welche über Router miteinander verbunden sind. | |
| | CONNTYPE | e | Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APNW - Access Point via Network: Access Point and central switch are located in different IP-Networks interconnected by routers. | |
| | LSRTADR | d | Adresse des Routers im HiPath 4000 LAN Segment VERBART=APNW: IP Adresse des Routers (Ports) im HiPath 4000 LAN Segment, über den der Access Point / das Netz, in dem sich der Access Point befindet, erreichbar ist. | |
| | LSRTADDR | e | Address of the Router in the HiPath 4000 LAN Segment CONNTYPE=APNW: IP address of the router (port) in the HiPath 4000 LAN Segment, via which the Access Point / the network, where the Access Point is located, is reachable. | |

Table 6

APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | APRTADDR | d | <p>Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht.</p> <p>VERBART=APNW: Über diesen Router muss der Access Point CC-A, CC-B, ADP und die HiPath HG 3500 Baugruppen im HiPath 4000 LAN Segment erreichen sowie alle anderen Access Points *).</p> <p>*) Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.</p> |
| | APRTADDR | e | <p>Address of the Router in the Access Point's Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network.</p> <p>CONNTYPE=APNW: Via this router the Access Point must be able to reach CC-A, CC-B, ADP and the HiPath HG 3500 boards in the HiPath 4000 LAN Segment as well as all other Access Points*).</p> <p>*) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.</p> |
| | STANDOID | d | <p>Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!</p> |

Table 6

APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | LOCID | e | Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already existing Access Point can be taken. System components in another room, floor or building are listed under a different location ID. |
| | STANDORT | d | Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden. |
| | LOCATION | e | Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed. |
| | TEL | d | Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann. |
| | PHONE | e | Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point. |
| | FAX | d | Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann. |
| | FAX | e | Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point. |
| | PLCHECK | d | Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Section 4.5, “Configuring Signaling Survivability”, on page 112 |

Table 6

APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | PLCHECK | e | <p>Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Section 4.5, “Configuring Signaling Survivability”, on page 112</p> |
| | ANZBKAN | d | <p>Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. -> Chapter 6, “Load Calculation”</p> |
| | BCHLCNT | e | <p>B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. -> Chapter 6, “Load Calculation”</p> |
| | KONVLAW | d | <p>Konvertierung von A-Law zu μ-Law bzw. μ-Law nach A-Law auf der HG 3575 Baugruppe. Das Leistungsmerkmal unterstützt nur Sätze nicht aber Teilnehmer, d.h. in einem derartig konfigurierten AP-Shelf dürfen nur Amtssätze eingerichtet sein!</p> |
| | CONVLAW | e | <p>Conversion from A-law to μ-law or μ-law to A-law on the HG 3575 board. The feature only supports trunks but not subscribers. This means, in such a shelf only the configuration of CO trunks is allowed!</p> |

Table 6

APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

APRT

With the AMO APRT, the access point is assigned its own IP address and, if desired, that of the TAP/Service PC link.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Enter IP addresses on the **IP Interface (NW)** tab and **Save**.



ADD-APRT:TYPE=APNET,LTU=99,APIPADR=192.168.23.99,
NETMASK=255.255.255.0,TAIPADDR=192.168.23.199;

NOTE: Prior to ADD-APRT, use **ping** to check that the IP addresses given to you by the administrator are reachable.

APIPADR and **TAIPADDR** must not respond, as this would indicate that the corresponding address had already been assigned.

APIPADR and **TAIPADDR** must be set differently for every access point. The AMO does not verify if this rule is observed.

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|--|
| APRT | APIPADR | d | Eigene IP-Adresse des Access Points VERBART*)=APNW: IP-Adresse des Access Points an dessen Ethernet-Port. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Table 5 "VERBART" on page 4-61 |
| | APIPADR | e | Own IP Address of the Access Point CONNTYPE*)=APNW: IP address of the Access Point's ethernet port. APIPADR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, ART=AP: siehe Table 5 "CONNTYPE" on page 4-61 |
| | NETMASK | d | Netzmaske des Netzes, dem APIPADR angehört |
| | NETMASK | e | Netmask of the network which APIPADR is part of |

Table 7

APNW: AMO APRT parameters in ADD branch under
TYPE=APNET

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | TAIPADR | d | IP-Adresse des TAP. Soll ein Techniker-Arbeitsplatz / Service PC zur (Fern)-Administration der HiPath 4000 am Access Point angeschlossen werden können, muss hier eine Adresse angegeben werden. Diese Adresse muss im gleichen Netz liegen, wie die APIPADR des Access Points. Wenn angeschlossen, tritt der TAP unter dieser Adresse an die UNIX Applikationen am ADP heran. TAIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. |
| | TAIPADDR | e | IP Address of the TAP. An address must be given if a TAP/Service PC for (remote) administration of the HiPath 4000 shall be connectable to the Access Point. This address must be in the same network as the APIPADR of the Access Point. When connected the service PC will access the UNIX applications on the ADP under this address. TAIPADDR must be different for every board. The AMO does not check compliance with this rule. |

Table 7

APNW: AMO APRT parameters in ADD branch under
TYPE=APNET

With the AMO APRT, additional functions of an access point can be configured. These are described in the respective chapters:

- Signaling survivability -> [Section 4.5, “Configuring Signaling Survability”, on page 112](#)
- Payload survivability - alternative routes -> [Section 4.8, “Configuring Payload Survability”, on page 149](#)
- Additional routes in the IP network which cannot/should not be accessible via the default router in the network of the access point or in the HiPath 4000 LAN segment -> [Section 4.4, “Configuring Special Routes”, on page 101](#)

STMIB

Nothing special has to be configured with STMIB. The CHANGE branches allow a multitude of parameters to be set. Details are described in [Section 4.2.3, “Changing Access Point Parameters with the AMO STMIB”, on page 80](#).

USSU

In order to actually put the access point into operation after the configuration process, it has to be activated.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu

and set the mode of action **Configure AP**, confirm with **OK**.



`EXEC-USSU:MODE=CONFAP, LTU=xx;`

From this moment on, the HiPath 4000 CC attempts to reach the access point and, as soon it achieves this, to start it.

NOTE: Prior to EXEC-USSU:CONFAP, the configuration must be updated on the system hard disk, Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with EXEC-USSU:UPDATAP, LTU number, UL.

In order to be able to reach the access point from the CC upon initial installation, various data has to be entered locally at the access point (see [Section 4.2.5, “Local Configuration of an Access Point”, on page 83](#)).

Configuring the IPDA Feature

Configuring an Access Point

4.2.2 Configuring a “Direct Link“ Access Point

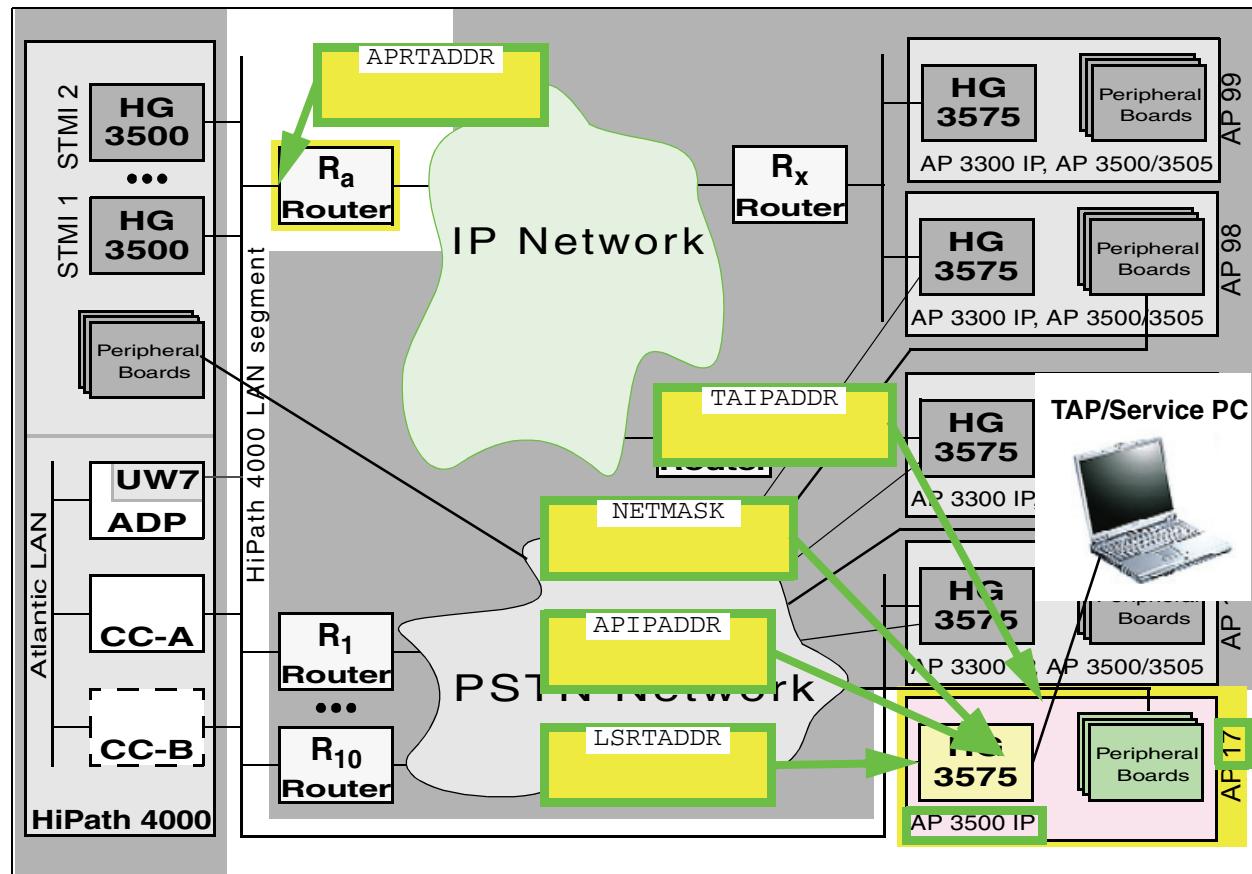


Figure 23 Configuring a “Direct Link” access point

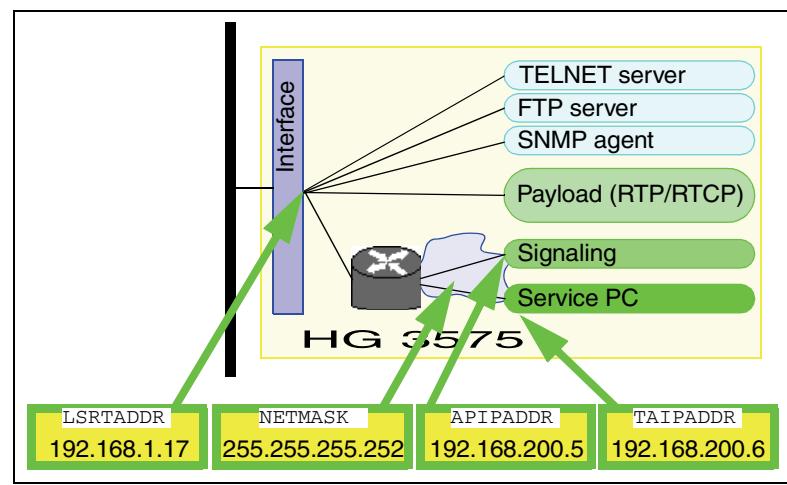


Figure 24 Internal address assignment of a “direct link” access point

ADD-UCSU: UNIT=AP, LTU=17,

| | |
|-------------------------|---|
| LTPARTNO=Q2302-X10 | SRCGRP=1, |
| FRMTYPE=INCH19, | CONNTYPE=APDL, |
| LSRTADDR=192.168.1.17, | APRTADDR=192.168.1.254, |
| LOCID=1, | LOCATION="MCH MACHTLFINGERSTR.1 GEB. 7202-111", |
| PHONE=08972223456, | FAX=08972265432, |
| PLCHECK=YES, | BCHLCNT=20, |
| CONVLAW=NO; | |
| <hr/> | |
| ADD-APRT: TYPE=APNET, | LTU=17, |
| APIPADDR=192.168.200.5, | NETMASK=255.255.255.252, |
| TAIPADDR=192.168.200.6; | |

In the case of a “direct link” access point, the Ethernet port of the access point is connected directly to the HiPath 4000 LAN segment and can be reached from CC-A and CC-B without a router.

However, the signaling survivability feature requires the re-routing of a link in the event of a fault (from LAN to modem). In order for this to function, the access point may not be “logically” present in the HiPath 4000 LAN segment. In this case, a router is activated within the access point which forwards the packets from the HiPath 4000 LAN to the “logical”, internal address of the access point.

To this end, the access point contains a “logical” IP network in which only itself and possibly the TAP/Service PC connection have an address. In order to save addresses, the netmask 255.255.255.252 can be used for this address.

Even these mini-networks and their addresses must be coordinated with the customer’s network administrator and, obviously, may not overlap.

[Figure 23 “Configuring a “Direct Link” access point](#) shows the following fundamental information required for configuring a direct link access point:

- The fact that the access point is linked with the HiPath 4000 LAN segment: Link type APDL, i.e. “direct link”.
- The LTU number of the access point, i.e. 17.
- The LTU part number specifies the HG 3575 used.
- The access point’s shelf type is derived from the type designation.
- The internal IP address of the access point: 192.168.200.5.
- The IP address for the TAP/Service PC link at the access point: 192.168.200.6.
- The IP address of the own Ethernet port via which the AP17 accesses the HiPath 4000 LAN segment: 192.168.1.17.

Configuring the IPDA Feature

Configuring an Access Point

- The netmask in the internal segment of the AP17: 255.255.255.252.
- The IP address of the router (port) at the HiPath 4000 LAN segment, via which the AP17 can reach access points which cannot be accessed directly at the HiPath 4000 LAN segment (that is “networked” APs), in this case router R_a: 192.168.1.254.
This router is omitted if there are no networked APs in the entire configuration or if this is an isolated demo installation. The default router **must** be configured with the zero address **0.0.0.0**.
- By limiting the number of B-channels, the bandwidth available to AP99 is indirectly reduced in the configuration example. This mechanism works independently of the bandwidth limitation performed by the Resource Manager in the “Large Enterprise Gatekeeper” Feature. For further information, please refer to [Chapter 6, “Load Calculation”](#).
- Should Payload Quality Handling be activated? For details see [Section 4.8, “Configuring Payload Survivability”, on page 149](#)
- The Source Group Index is explained in detail in [Section 4.7, “Configuring Source Dependent Routing”, on page 145](#).

Additional data is explained in more detail with the corresponding AMO parameters.

Generation

An access point is configured with three AMOs (UCSU, APRT, STMIB) and activated with USSU.

UCSU

With the AMO UCSU, the access point is configured as a new shelf in the system and its reachability via routers is ensured.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **New** and enter the LTU of the access point.
Enter the relevant data on the **General** and **IP Interface (DL)** (Connect Type=APDL) tab and **Save**.



```
ADD-UCSU:UNIT=AP,LTU=17,LTPARTNO=Q2302-X10,SRCGRP=1,FRMTYPE=INCH19,CONNTYPE=APDL,LSRTADDR=192.168.1.17,APRTADDR=192.168.1.254,LOCID=1,LOCATION="M CH MACHTLFINGERSTR.1 GEB. 7202-111",PHONE=08972223456,FAX=08972265432,PLCHECK=YES,BC HLCNT=20,CONVLAW=NO;
```

The parameters FRMTYPE and CONNTYPE cannot be changed after the ADD!

NOTE: Prior to ADD-UCSU, use **ping** to check that the IP addresses given to you by the administrator are reachable.

APRTADDR must respond.

LSRTADDR must not respond, as this would indicate that the corresponding

address had already been assigned.

LSRTADDR must be set differently for every “direct link” access point. The AMO does not verify if this rule is observed.

NOTE: Routing to the access points, which is configured for CC-A or CC-B, must also be configured in the UW7 for the TAP/Service PC link.

With “direct link” access points, the internal AP router must be taken into account in the UW7. In other words, routing entries are required for
Host=APRT:TAIPADDR,
Netmask=APRT:NETMASK,Router=UCSU:LSRTADDR.

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|--|
| UCSU | LTSACHNR | d | Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/NCUI4. |
| | LTPARTNO | e | Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used. |
| | SRCGRP | d | Source Group Index Zuordnung des Access Points in eine Source Group für “Source Dependent Routing”. (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben. |
| | SRCGRP | e | Source Group Index Assignment of the Access Point to a Source Group for “Source Dependent Routing”. This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there. |
| | FRAMETYP | d | Typ des LTU-Rahmens (Shelf Typ) |
| | | AP-Typ | FRAMETYP |
| | | AP 3300 IP | L80XF |
| | | AP 3500 IP | INCH19 |
| | | AP 3700 IP | AP37009 |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|---|
| | FRMTYPE | e | Type of the LTU Frame (Shelf Type) |
| | | | AP-Type FRAMETYPE |
| | | | AP 3300 L80XF IP |
| | | | AP 3500 INCH19 IP |
| | | | AP 3700 AP37009 IP |
| | VERBART | d | Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APDL - Access Point Direct Link: - Access Point ist direkt am HiPath 4000 LAN Segment angeschlossen, d.h. im selben IP-Netz. |
| | CONNTYPE | e | Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APDL - Access Point Direct Link: - Access Point is connected directly to the HiPath 4000 LAN Segment, i.e. in the same IP network. |
| | LSRTADR | d | Adresse des Routers im HiPath 4000 LAN Segment VERBART=APDL: Dies ist die IP-Adresse am Ethernet-Port des Access Points, über den er mit dem HiPath 4000 LAN Segment verbunden ist. Bei APDL enthält der Access Point einen lokalen Router der die IP-Adresse des Access Points (in einem eigenen Netzwerksegment) mit dem HiPath 4000 LAN Segment verbindet. D.h. auch hier handelt es sich um die Adresse eines (wenn auch unsichtbaren) Routers. Diese IP-Adresse muss zum HiPath 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO). LSRTADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | LSRTADR | e | <p>Address of the Router in the HiPath 4000 LAN Segment CONNTYPE=APDL: This is the IP address of the Access Point's ethernet port connected to the HiPath 4000 LAN Segment. With APDL the AP contains a local router that connects the own IP address of the Access Point (in its own network segment) to the HiPath 4000 LAN Segment. It's a router's address, even with the router invisible. This IP address must belong to the HiPath 4000 LAN Segment (see NETADDR in AMO SIPCO) LSRTADDR must be different for every board. The AMO does not check compliance with this rule.</p> |
| | APRTADR | d | <p>Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht. VERBART=APDL: Über diesen Router muss der direkt am HiPath 4000 LAN Segment angeschlossene Access Point alle Access Points erreichen, die sich in anderen Netzen befinden. Meist ist dies der Default-Router des HiPath 4000 LAN Segments, welcher mit dem Parameter DEFRT im AMO SIPCO eingerichtet wird*). Sind in der gesamten Konfiguration keine "networked" APs enthalten, oder ist dies eine isolierte Demo-Installation, so enfällt dieser Router. Geben Sie dazu hier die Null-Adresse 0.0.0.0 an.</p> <p>*)Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.</p> |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|---|
| | APRTADDR | e | <p>Address of the Router in the Access Point's Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network.</p> <p>CONNTYPE=APDL: Via this router an Access Point directly connected to the HiPath 4000 LAN Segment must be able to reach all Access Points that are located in different networks. Usually this is the default router of the HiPath 4000 LAN Segment, administered in parameter DEFRT with AMO SIPCO*).</p> <p>If there are no "networked" APs in the whole configuration or if this is a stand-alone demo installation, this router is not needed. Give the address 0.0.0.0 for this purpose.</p> <p>*) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.</p> |
| | STANDOID | d | <p>Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!</p> |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | LOCID | e | Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already existing Access Point can be taken. System components in another room, floor or building are listed under a different location ID. |
| | STANDORT | d | Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden. |
| | LOCATION | e | Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed. |
| | TEL | d | Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann. |
| | PHONE | e | Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point. |
| | FAX | d | Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann. |
| | FAX | e | Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point. |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | PLCHECK | d | <p>Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Section 4.5, "Configuring Signaling Survivability", on page 112</p> |
| | PLCHECK | e | <p>Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Section 4.5, "Configuring Signaling Survivability", on page 112</p> |
| | ANZBKAN | d | <p>Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. -> Chapter 6, "Load Calculation"</p> |
| | BCHLCNT | e | <p>B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. -> Chapter 6, "Load Calculation"</p> |
| | KONVLAW | d | <p>Konvertierung von A-Law zu μ-Law bzw. μ-Law nach A-Law auf der HG 3575 Baugruppe. Das Leistungsmerkmal unterstützt nur Sätze nicht aber Teilnehmer, d.h. in einem derartig konfigurierten AP-Shelf dürfen nur Amtssätze eingerichtet sein!</p> |
| | CONVLAW | e | <p>Conversion from A-law to μ-law or μ-law to A-law on the HG 3575 board The feature only supports trunks but not subscribers. This means, in such a shelf only the configuration of CO trunks is allowed!</p> |

Table 8

APNW: AMO UCSU parameters in ADD branch under ART=AP

APRT

With the AMO APRT, the access point is assigned its own (internal) IP address and, if desired, that of the TAP/Service PC link.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Enter IP addresses on the **IP Interface (DL)** tab and **Save**.



ADD-APRT:TYPE=APNET,LTU=17,APIPADR=192.168.200.5,
NETMASK=255.255.255.252,TAIPADDR=192.168.200.6;

NOTE: If you want to check the (internal) **APIPADR** and **TAIPADDR** IP addresses after startup using **ping**, you must configure the route to the AP internal network segment on the computer from which the **ping** is dispatched.
=> Host=APRT:APIPADR, Netmask=APRT:NETMASK,
Router=UCSU:LSRTADDR.

APIPADR and **TAIPADDR** must be set differently for every access point. The AMO does not verify if this rule is observed.

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|---|
| APRT | APIPADR | d | Eigene IP-Adresse des Access Points VERBART*)=APDL: IP-Adresse des Access Points in seinem eigenen Netzwerksegment - nicht die IP-Adresse der Ethernet-Ports, welche in diesem Fall vom internen Router belegt wird. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Table 5 on page 61 |
| | APIPADR | e | Own IP Address of the Access Point CONNTYPE*)=APDL: IP address of the Access Point in its own network segment - not the IP address of its ethernet port which is assigned to the internal router in this case. APIPADR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, UNIT=AP: siehe Table 5 "CONNTYPE" on page 4-61 |
| | NETMASK | d | Netzmaske des Netzes, dem APIPADR angehört |
| | NETMASK | e | Netmask of the network which APIPADR is part of |

Table 9

APDL: AMO APRT parameters in ADD branch under TYPE=APNET

Configuring the IPDA Feature

Configuring an Access Point

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|---|
| | TAIPADDR | d | IP-Adresse des TAP. Soll ein Techniker-Arbeitsplatz / Service PC zur (Fern)-Administration der HiPath 4000 am Access Point angeschlossen werden können, muss hier eine Adresse angegeben werden. Diese Adresse muss im gleichen Netz liegen, wie die APIPADR des Access Points. Wenn angeschlossen, tritt der TAP unter dieser Adresse an die UNIX Applikationen am ADP heran. Beachten Sie den Hinweis in Section 4.2.2, “UCSU”, on page 70 . TAIPADDR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. |
| | TAIPADDR | e | IP Address of the TAP. An address must be given if a TAP/Service PC for (remote) administration of the HiPath 4000 shall be connectable to the Access Point. This address must be in the same network as the APIPADR of the Access Point. When connected the service PC will access the UNIX applications on the ADP under this address. Please observe the advice in Section 4.2.2, “UCSU”, on page 70 TAIPADDR must be different for every board. The AMO does not check compliance with this rule. |

Table 9

APDL: AMO APRT parameters in ADD branch under TYPE=APNET

With the AMO APRT, additional functions of an access point can be configured. These are described in the respective chapters:

- Signaling survivability -> [Section 4.5, “Configuring Signaling Survivability”, on page 112](#)
- Payload survivability - alternative routes -> [Section 4.8, “Configuring Payload Survivability”, on page 149](#)
- Additional routes in the IP network which cannot/should not be accessible via the default router in the network of the access point or in the HiPath 4000 LAN segment -> [Section 4.4, “Configuring Special Routes”, on page 101](#)

STMIB

Nothing special has to be configured with STMIB. The CHANGE branches allow a multitude of parameters to be set. Details are described in [Section 4.2.3, “Changing Access Point Parameters with the AMO STMIB”, on page 80](#).

USSU

In order to actually put the access point into operation after the configuration process, it has to be activated.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu

and set the mode of action **Configure AP**, confirm with **OK**.



EXEC-USSU:MODE=CONFAP,LTU=xx;

From this moment on, the HiPath 4000 CC attempts to reach the access point and, as soon it achieves this, to start it.

NOTE: Prior to EXEC-USSU:CONFAP, the configuration must be updated on the system hard disk, Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with EXEC-USSU:UPDATAP, LTU number , UL.

In order to be able to reach the access point from the CC upon initial installation, various data has to be entered locally at the access point (see [Section 4.2.5, “Local Configuration of an Access Point”, on page 83](#)).

Configuring the IPDA Feature

Configuring an Access Point

4.2.3 Changing Access Point Parameters with the AMO STMIB

Please refer to [Chapter 12, “HiPath Gateway HG 3575 V4 - Changing Parameters with AMO STMIB”](#) in the document “HiPath Gateways HG 3500 and HG 3575”.

4.2.4 Deleting an Access Point

If an access point is to be removed from the configuration (in the example: AP 43), the following sequence must be complied with:

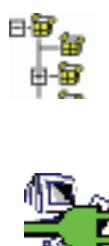
- If payload survivability is configured, it must first be checked whether the access point to be deleted provides the trunk access for a source group. If it does, a suitable replacement must be found.
- If payload survivability is configured and a source group becomes superfluous when an access point is deleted, the LCR must be adapted and the source group deleted if necessary.



**Configuration Management --> System Data --> IPDA
--> IPDA - Payload Survivability**
Click **Search**, select the access point and **Delete**.

`DELETE-APRT:TYPE=ALTROUT, SRCGRP=3;`

- Deletion of all peripheral modules configured within this access point (presupposes that no subscribers are configured on that module, etc.)
- If signaling survivability is configured for this access point:
([Section 4.5, “Configuring Signaling Survivability”, on page 112](#))
 - Delete the assignment of this access point to a survivability router



**Configuration Management --> System Data --> IPDA --> IPDA
Access Point**
Click **Search** and select the access point.
Delete the desired router number on the **General** tab under **Signaling
Survivability** and **Save**.

`DELETE-APRT:TYPE=SURV, CONF=AP, LTU=43;`

- If special routes are configured:
([Section 4.4, “Configuring Special Routes”, on page 101](#))
 - Delete the corresponding entries in the routing tables of other access points, if these entries lose their validity for additional access points.

In the example in [Figure 28 “Special routes between access points”](#), the route via Router R₂ becomes superfluous if AP 43 is deleted. If, however, AP 98 was deleted instead of AP 43, the route would have to remain in place, as it is also valid for AP 99.



**Configuration Management --> System Data --> IPDA --> HG3575
Additional Routing**

Click **Search** and select the access point.

Enter zero addresses (0.0.0.0) in the lines of the routing table that are to be deleted and **Save**.

Configuring the IPDA Feature

Configuring an Access Point



DEL-APRT:TYPE=ROUTTBL, MTYPE=NCUI, LTU=99, INDEX=1;
Note: No distinction is made here between hardware types. NCUI applies to NCUI2 and NCUI4.

- Deactivating the access point with USSU:



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.
Click **Deactivate** on the **Action** pull-down menu.



DEACTIVATE-USSU:LTU=43 ;

- Deactivating the IP connection of the access point with USSU:



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



EXEC-USSU:MODE=DELAP, LTU=43 ;

- Deleting the access point (CM):



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point, then click **Delete**.

- Deleting the IP network configuration of the access point:



DELETE-APRT:TYPE=APNET, LTU=43 ;

- Deleting the access point with UCSU:



DELETE-UCSU:UNIT=AP, LTU=43 ;

NOTE: If the removed access point was configured for AP Emergency (i.e. it was assigned an emergency group), you must observe the following:
The IP address of the removed access point can only be reused when this change has been saved on all CC APs, in other words, when “cloning” is completed using HiPath Backup & Restore.

4.2.5 Local Configuration of an Access Point

If an access point has been configured in the HiPath 4000 switch, it cannot be put into operation immediately. The central system cannot establish contact with the access point until this has been configured with the essential IP addresses, etc.

A "HiPath 4000 Expert Access" application is available in order to perform this initial access point configuration locally. To this end, the TAP/Service PC is connected to the RS232/V.24 interface of the HiPath HG 3575 with the designation "Service" and the application started.

The terminal login must be used for login purposes. In the case of virgin modules, this is "TRM", and no password is set. If the module has already been in operation and the terminal login and password have been changed, these later values apply.

If there is a duplex processor (CC-B) in the HiPath 4000 switch, the address must always be specified. After all, it is not possible to predict whether CC-A or CC-B will be playing the active role at this time. If there is no CC-B in the system, the IP address for this processor is not needed.

The IP address of the TAP need only be specified if the administration function of the HiPath 4000 switch is to be accessed from this access point.

If VLAN tagging is used in the Ethernet segment to which the access point should be connected, a setting must be performed for it during initial startup.

If the access point was operated in a network with VLAN tagging and should now run without VLAN tagging, this setting must also be changed locally.

If the access point is to be operated with fixed Ethernet interface settings for bit rate and mode or if this fixed setting is to be removed (in the event of relocation to another network), this setting too must be performed locally.

Of the parameters which are displayed and adjustable, only a certain number actually have to be entered. All other parameters are loaded from the HiPath 4000 switch as soon as the central system can establish contact with the access point;

NOTE: Changing a parameter value locally does **not** result in a change of the value in the system.

Absolutely all parameters configured locally at the access point are overwritten by the values configured in the system upon loading the module from the HiPath 4000 switch.

When configuring the access point locally, a distinction is again also made between "networked" and "direct link".

Networked access point

The following fields must be completed:

Configuring the IPDA Feature

Configuring an Access Point

| Parameter | Note | AMO - Zweig - Parameter |
|---|---|---|
| IP address of the access point | May not be in the same network as the IP address of the CC-A | APRT TYPE=APNET - APIPADDR |
| Netmask in the network of the access point | The netmask must match the IP address class of the access point. | APRT TYPE=APNET - NETMASK |
| IP address of the default router in the network of the access point | Must be in the same network as the IP address of the access point | UCSU UNIT=AP - APRTADDR |
| IP address of the CC-A | | SIPCO TYPE=LSNET - CCAADDR |
| IP address of the CC-B | Must be in the same network as the IP address of the CC-A | SIPCO TYPE=LSNET - CCBADDR |
| Netmask of the HiPath 4000 LAN segment | The netmask must match the IP address class of the CC-A. | SIPCO TYPE=LSNET - NETMASK |
| IP address for TAP link | Must be in the same network as the IP address of the access point | APRT TYPE=APNET - TAIPADDR |
| VLAN tagging on/off | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN |
| VLAN ID | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID |
| Ethernet interface operating mode | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE |

Table 10 Basic initialization parameters for “networked” access points

Direct link access point

The following fields must be completed:

| Parameter | Note | AMO - Branch - Parameter |
|---|---|----------------------------|
| IP address of the access point in the HiPath 4000 LAN segment | Must be in the same network as the IP address of the CC-A | UCSU UNIT=AP - LSRTADDR |

Table 11 Basic initialization parameters for “direct link” access point

| Parameter | Note | AMO - Branch - Parameter |
|---|---|---|
| HiPath 4000 LAN segment Netmask | The netmask must match the IP address class of the CC-A. | SIPCO TYPE=LSNET - NETMASK |
| IP address of the default router in the HiPath 4000 LAN segment | Must be in the same network as the IP address of the CC-A | UCSU UNIT=AP - APRTADDR |
| IP address of the CC-A | | SIPCO TYPE=LSNET - CCAADDR |
| IP address of the CC-B | Must be in the same network as the IP address of the CC-A | SIPCO TYPE=LSNET - CCBADDR |
| IP address of the access point in the internal AP network segment | May not be in the same network as the IP address of the CC-A | APRT TYPE=APNET - APIPADR |
| Netmask of the internal AP network segment | The netmask must match the IP address class of the access point in the internal AP network segment. | APRT TYPE=APNET - NETMASK |
| IP address for TAP link | Must be in the internal AP network segment. | APRT TYPE=APNET - TAIPADDR |
| VLAN tagging on/off | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN |
| VLAN ID | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID |
| Ethernet interface operating mode | | STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE |

Table 11 Basic initialization parameters for “direct link” access point

Information on local configuration without the “HiPath 4000 Expert Access” application can be found in [Chapter 7, “Local Access Point Administration at CLI via Terminal”](#).

4.2.6 Reference Clock in Access Point

The HiPath 4000 central system has a highly precise clock generator which can be synchronized from various sources. Possible sources include, for instance, digital trunk circuits. The corresponding connection modules can then supply the clock timing in the LTUs 1-15 and synchronize the central clock generator. The AMO REFTA is responsible for configuring which circuits can be used as reference clock suppliers and querying which supplier is currently active.

Access Points of the type HiPath AP 3300 IP, AP 3500 IP or AP 3700 IP are connected in asynchronous fashion via the IP network. Thus, the central clock generator cannot be synchronized from LTUs 17-99.

On account of this asynchronous connection, the access point itself is also unable to be synchronized from the central clock generator. Therefore, the HiPath HG 3575 module of the access point is equipped with its own highly precise clock generator.

The asynchronism of the clock generators in the HiPath 4000 central system and in the various access points has no interfering effect on the communication between these components. The jitter buffers required for voice transmission also compensate smoothly for the slight slip between the clock generators.

However, if digital trunk or tie trunk circuits are operated in an access point, the local clock generator must be synchronized with the network clock ("CO Clock").

To this end, management of the reference clock has been extended with the AMO REFTA. The basic principle is simple:

- Reference clock sources in LTUs 1-15 are used to synchronize the central clock generator.
- Reference clock sources in LTUs 17-99 are used to synchronize the local clock generators in the respective access point.

Thus, in a HiPath 4000 switch with 83 access points of the type HiPath AP 3300 IP or AP 3500 IP, the synchronization of 84 clock generators has to be managed. This means that 84 active clock suppliers (central unit + 83 access points) may exist in such a system.

4.2.7 Loading New Loadware on a HiPath HG 3575

From HiPath 4000 V4 on a new load concept via HTTPS has been developed for HG 3575 and HG 3500. Please refer to „HiPath Gateways HG 3500 and HG 3575“, [Chapter 7, “Load Concept for Gateway Boards”](#).

The loadware for a HG 3575 is very extensive. If, while the module is being loaded, it is determined that the loadware in the flash memory of the module does not match the loadware stored in the hard disk of the HiPath 4000 central system, the loadware is reloaded on the HG 3575.

The loadware is transferred via FTP, with the HG 3575 downloading the loadware from the FTP server of the HiPath 4000 central processor (in the RMX system).

The FTP server can only transfer loadware to one HG 3575 at a time. If there are multiple HG 3575s in the system (up to 83 are possible), the other modules wait their turn. This takes quite a long time and considerably slows down startup of the system.

It is therefore possible for a HG 3575 to download new loadware from the FTP server while the system is running, without executing it immediately. Actions of this type should be performed at off-peak times, as the loadware transfer reduces the bandwidth for signaling messages. The load operation can also be performed with signaling survivability. The effect on the available bandwidth is particularly critical in this case.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu and select the mode of action **Background Loading of NCUI LW Files**, select **LW** under **Files to be Loaded** and confirm with **OK**.



`EXEC-USSU:MODE=NCUILOAD,LTU=xx,FILES=LW;`
If the LTU number is not specified, all HG 3575s that are ready (READY) at this time are loaded.

SIU files can also be loaded in this way.

FILE=

| | |
|------------|---------------------------|
| SIUTONES | TONES |
| SIURECV | SIU-RECEIVERS |
| SIUANN | SIU-ANNOUNCEMENTS |
| SIUMOH | SIU -MUSIC ON HOLD |
| SIUTDS | SIU -TDS |
| LW | LW file -- NCUI |
| ALLSIU | All possible SIUs |
| ALL | All loadable files |

Configuring the IPDA Feature

Configuring an Access Point

To apply the loadware while the system is active, the following actions are required:



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Click **Deactivate** on the **Action** pull-down menu.

Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.



DEACTIVATE-USU:LTG=1,LTU=xx;
ACTIVATE-USU:UNIT=LTG,LTG=1,LTU=xx;

NOTE: Connections are cleared down without further warning.

Changing the music on hold (MOH) in the system (AMO ZAND:MELODY=X)

When changing the MELODY setting, the following command sequence must be executed (for each AP) so that the changes become effective immediately:



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Click **Deactivate** on the **Action** pull-down menu.

Once the system has confirmed deactivation of the AP, reactivate it with **Activate**.



DEACTIVATE-USU:LTG=1,LTU=xx;
ACTIVATE-USU:UNIT=LTG,LTG=1,LTU=xx;

4.2.8 Updating Access Point Loadware during an RMX Upgrade (New Fix Release/Minor Release)

HiPath 4000 V4 Release 1.7 supports "AP multicast loading". This feature lets you perform simultaneous loading operations for multiple access points. Originally, simultaneous loading operations were only possible for access points containing boards that already featured the latest loadware. In Release 1.7 and higher, this form of loading is also possible if the boards need new loadware.

Prerequisite

The system to be upgraded has at least HiPath 4000 V4 R1.7 software.

Procedure

1. Use the traditional FTP solution to transfer the new loadware for the HG 3575 to the access point (up to five access points per run). See also [Section 4.2.7, "Loading New Loadware on a HiPath HG 3575"](#).

Once the new loadware has been successfully transferred and activated, the TCP/IP connection is re-established between the HiPath Host System (HSR) and the access point.

The system must be warm-booted and a golden loadware check must be successfully performed to transfer the loadware downloaded in the background to the NCUI.

This is accomplished either

- with the AMO USSU (specific deactivation/activation) or
- by warm-booting the NCUI after link failure (ALVTIME) or
- by performing a specific restart with the HiPath after the loadware transfer during an RMX upgrade.

The restart (warm boot) with the new loadware is followed by a golden loadware check with a 60-minute timeout. If this golden loadware check fails, the NCUI restarts with the old loadware and, where applicable, the new loadware (HD) is retransmitted.

NOTE: This step is skipped if there is no new loadware available for the HG 3575.

2. The loadware transfer for the peripheral boards starts.
3. The access points are entered in the load list once the loadware has been transferred.

Configuring the IPDA Feature

Configuring an Access Point

4. The first access point in the load list is put into full operation immediately (takes approx. 15 minutes). While this access point is being put into operation, other access points that have already completed the loadware transfer/activation are entered in the load list.
5. As soon as the first access point has gone into operation, all access points that have been entered in the load list in the meantime are simultaneously loaded and put into operation.

NOTE: In the past, the APs in the load list were processed or put into operation in sequential order.

6. While these access points are being put into operation, other access points that have completed loadware transfer/activation are entered in the load list.
7. As soon as the access points have gone into operation, all access points grouped together on the load list are put into operation simultaneously.
8. These procedures are repeated until all access points have been upgraded.

4.2.9 Information on Exchanging HiPath HG 3575 Boards

The following must be observed when exchanging a HG 3575 board in a system:

- The HG 3575 board must not be powered on or plugged in.
- The new board must be configured with the same basic configuration as the old board (IP addresses, etc.).
To do this, the configuration of the old board can be read out using “HiPath 4000 Expert Access” and stored on a file with which the new board can be configured.
If this is no longer possible with the old board, the data must be taken from the system configuration.
- Every HG 3575 board has an individual Ethernet MAC address. The MAC address which is visible from the network changes when boards are changed.

NOTE: Please inform the network carrier of the change. The network provider needs the MAC addresses to find devices involved in IP address conflicts.

The board's MAC address can be found on the sticker on the solder side of the printed circuit board.

- The following AMO action must be performed once the module has been booted:



Unconditional loading can only be initiated in expert mode.
Expert Mode --> “HiPath 4000 Expert Access” --> Open ...<IP> with AMO (see AMO command)

EXEC-USSU:UPDATAP , LTU=<number> , UL;

This ensures that the entire system configuration data is written to the module. The access point is thus restarted and is booted using the latest data. This is necessary as the system does not always detect that the board was exchanged.

This process is also required if the same board was removed from the system, reconfigured locally and put back in the same position in the system.

For more information on exchanging HG 3575 boards refer to document „HiPath Gateways HG 3500 and HG 3575“, [Section 4.2.3, “Exchanging Boards”](#)).

4.2.10 Information on the 19“ HiPath AP 3500 IP Access Point

[Figure 25](#) shows the front view of a HiPath AP 3500 IP. The shelf can be mounted in a 19“ rack using additional angle brackets and has a height of 3HE.

There is space on the left for 4 modules and the topmost slot is allocated to the HiPath HG 3575 (NCUI2/4). Peripheral modules of the HiPath 4000 can be inserted into the other slots. These modules are covered by a metal panel that is inserted separately. In the figure, this panel has been removed from the bottom slot.

At the rear, either the usual main distribution cables can be attached or plug-in patch panels can be used to connect the devices directly using Western plugs.

In addition to the modules, the rack also contains 2 power supply modules on top of one another. The AP 3500 IP can be operated using a power supply module. A second may also be operated as a redundant unit.

A ventilator module is located at the right-hand side. Because the modules are in a horizontal position, the system has to be forced ventilated.

NOTE: The ventilation openings on the left and right-hand side of the housing must not be obstructed. The operating position of the equipment is horizontal.

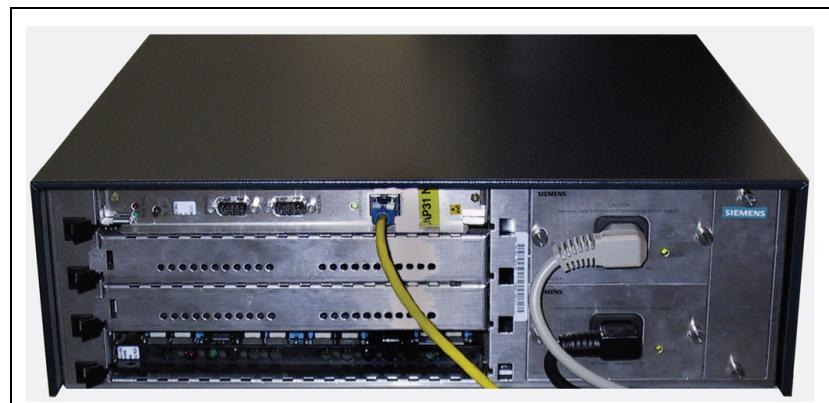


Figure 25 HiPath AP 3500 IP - front view

The HiPath AP 3500 IP can be extended by four slots using a HiPath AP 3505 IP with a similar structure (no HG 3575 in the AP 3505).

Special features

- The AP 3500 IP represents the left and the optional AP 3505 IP represents the right half of a conventional shelf.

- The slots are counted from bottom up and are numbered 1,2,3 and 4 in the AP 3500 IP
(4 is HG 3575), and 5,6,7 and 8 in the optional AP 3505 IP.
- Boards with front connectors can only be used if they are fitted with a suitable metal panel (for example, STMI2, DIUN2 starting with status -X-7, SLC24 starting with status -X200-9, PBXXX starting with status -X-F3, ...)
- SIVAPAC modules with adapters are not supported, because they do not fit under the shielding cover. As an exception, a number of these boards are fitted with a new plastic panel C39228-A402-C21. (TMEW2, SLMA,TMDID,TMEMUS).

4.2.11 Information on the 19“ HiPath AP 3700 IP Access Point

Figure 26 HiPath AP 3700 IP - front view on page 4-95 shows the front view of a HiPath AP 3700 IP. The frame can be installed in 19“ cabinets. For this, it must be set on sliding rails/mounting rails installed in the cabinet and terminated at the cabinet uprights by means of the 19“ mounting bracket supplied.

AP 3700 IP required a height of 11 HE (10 HE + 1 HE play).

NOTE: AP 3700 IP is not forced ventilated and consequently, does not feature a fan.

For installation, please pay particular attention to requirements in terms of air supply and minimum air volume specified in the installation instructions.

The left half of the shelf can accommodate five peripheral boards (slot 1 to 5). HG 3575-2 (NCUI2) is only supported on the central slot (slot 6), not HG 3575 from HiPath version 1. The correct shelf half accommodates four peripheral boards (slot 7 to 10).

If the peripheral boards are not already equipped with a suitable metal panel (for example, STMI2, see [Figure 26](#), slot 4 and 9), they are covered by a metal panel that is inserted separately. (on slot 1 and 2 in the diagram). Unused slots must be covered by a metal panel and guarantee the necessary level of shielding.

Boards with front connectors can only be used if they are fitted with a suitable metal panel (for example, STMI2, DIUN2 starting with status -X-7, SLC24 starting with status -X200-9, PBXXX starting with status -X-F3, ...)

SIVAPAC modules with adapters are not supported, because they do not fit under the shielding cover. As an exception, a number of these boards are fitted with a new plastic panel C39228-A402-C21. (TMEW2, SLMA,TMDID,TMEMUS).

The project planning guideline's instructions on the installation of peripheral boards should therefore be followed precisely.

At the rear, either the usual main distribution cables can be attached or plug-in patch panels can be used to connect the devices directly using Western plugs.

Up to three power supply modules can be connected side by side under the board. Two modules are sufficient for supplying the maximum configuration. A third module may also be connected as a redundant unit.

The power supply modules can be connected to the 115/230 V alternating current or 48 V direct current. The three modules are fed over a shared connected at the rear of the housing.

The right part of the AP 3700 IP can accommodate a survivability unit, a cPCI cassette with a standalone emergency control unit.

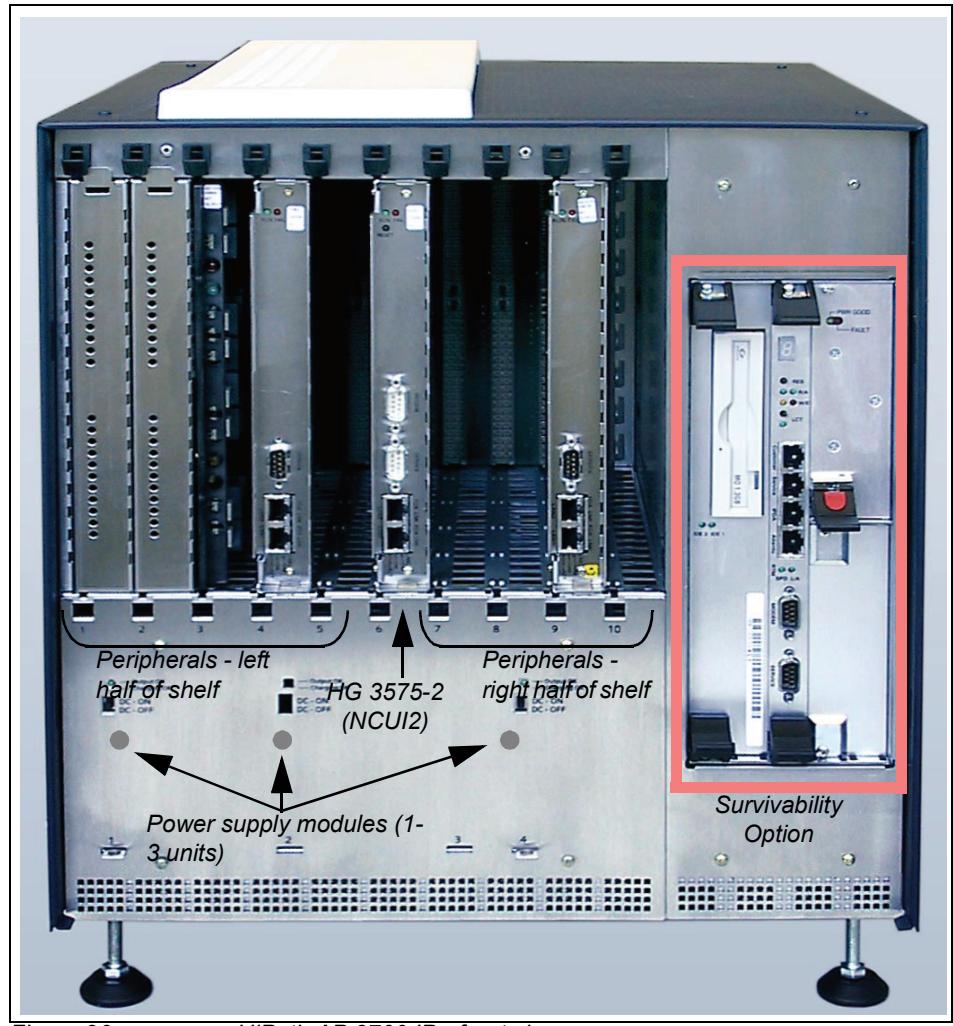


Figure 26

HiPath AP 3700 IP - front view

Configuring the IPDA Feature

Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 System

4.3 Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 System

For more information on HG 3500 gateway please refer to „HiPath Gateways HG 3500 and HG 3575“.

The common gateway HG 3500 - added as HG3570 - establishes the payload connections between the central HiPath 4000 system and the access points distributed within the framework of the IP distributed architecture.

- HiPath HG 3500 gateways, configured as HG 3570, may only be used in the peripheral shelves (LTU 1-15) of the central system.
- The time slots required by the HG 3570 gateways in a half shelf must be nonblocking. The maximum number of B channels supported by the board hardware can be reduced using the BCHLCNT command in the AMO BFDAT.
- Every shelf in which a HiPath HG 3570 is installed must be equipped with an LTUCX module. Use in the base shelf of the HiPath 4300 is permitted.
- Up to 83 HG 3570 gateways can be used in a HiPath 4000 system. The payload connections between the central HiPath 4000 system and the access points are distributed evenly across all HG 3500s.
- There is no assignment of payload connections from HG 3575 to HG 3500. The number of HG 3500s in the system is based on the traffic volume, not on the number of access points. If one HG 3500 fails, it is not assigned any new calls. The other available HG 3500s take on the payload.

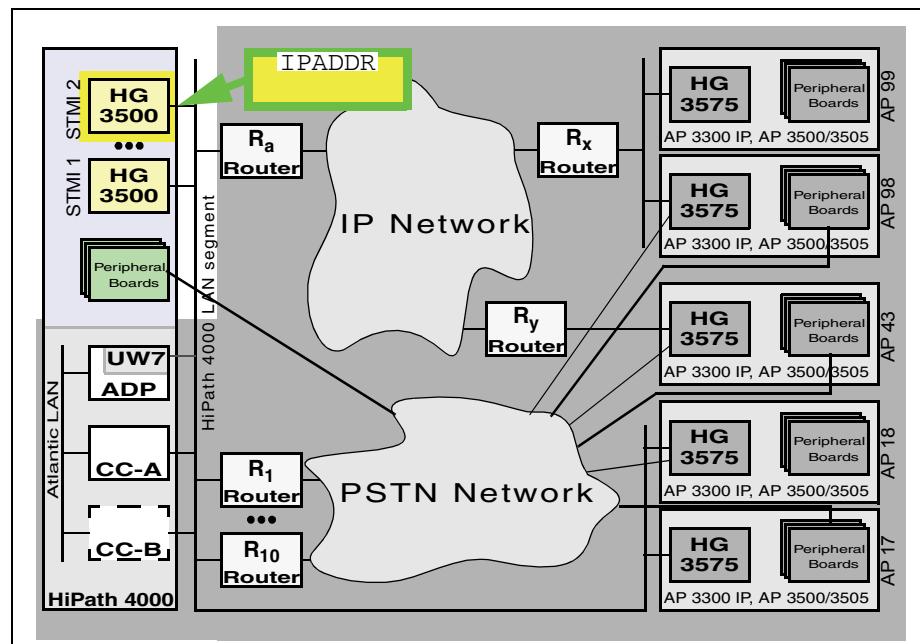


Figure 27

Configuring a HiPath HG 3500 for IPDA

| | | |
|---------------|--|--|
| ADD-BFDAT: | FCTBLK=1 , BRDBCHL=BCHL60&BCHL120 ; | FUNCTION=HG3570 , |
| CHANGE-BFDAT: | CONFIG=CONT , FUNCTION=HG3570 , | FCTBLK=1 , BCHLCNT=40 ; |
| CHANGE-BFDAT: | CONFIG=OK , ANSW=YES ; | FCTBLK=1 , |
| ADD-BCSU: | MTYPE=IPGW , SLOT=91 , FCTID=1 , IPADR=192.168.1.11 , | LTU=5 , PARTNO=Q2316-X , FCTBLK=1 , BKAN3570=40 ; |
| CHNAGE-BCSU: | TYPE=HWYBDL , SLOT=91 , HWYBDL=A ; | LTU=5 , PARTNO=Q2316-X , |

Generation

A HiPath HG 3500 module with FUNCTION=HG3570 is configured with 3 AMOs: AMO BFDAT, AMO BCSU and AMO CGWB.

However, AMO CGWB is only needed if additional routes in the IP network are required in addition to the default router in the HiPath 4000 LAN segment. Please refer to [Section 4.4, “Configuring Special Routes”, on page 101](#).

BFDAT

Configuration of the functional blocks for common gateway boards for IPDA.



Configuration Management --> System Data --> Board --> CGW Function Block

Click **New**, enter data and click **Save**.



ADD-BFDAT:FCTBLK=1 , FUNCTION=HG3570 , BRDBCHL=NCHL&BCHL ;

CHA-

BFDAT:CONFIG=CONT , FCTBLK=1 , FUNCTION=HG3570 , BCHLCNT=40 ;

CHNAGE-BFDAT:CONFIG=OK , FCTBLK=1 , ANSW=YES ;

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|--|
| BFDAT | ANZBKAN | d | Anzahl der funktionsbezogenen B-Kanäle. |
| | BCHLCNT | e | Defines the number of b-channels related to the selected function. |
| | ANTW | d | JA: Block-KOnfiguration abschließen |
| | ANSW | e | YES: Finish block configuration |
| | BGBKAN | d | Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen |

Configuring the IPDA Feature

Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 System

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|--|
| | BRDBCHL | e | Dedicates the block for boards with 60 and/or 120 b-channels. |
| | CONFIG | d | WEITER: Weitere Block-Konfiguration möglich OK: Block-Konfiguration abschließen |
| | CONFIG | e | CONT: Continue block configuration OK: Finish block configuration |
| | FCTBLK | d | Dieser Index beschreibt den Funktionsblock welcher auf dem CGW konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten physikalischen Lines (Sätze der Baugruppe) festgelegt. |
| | FCTBLK | e | This index describes the function block which should be configured on the CGW board. With that index the amount of needed physical lines (board circuits) is calculated. |
| | FUNCTION | d | Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die benötigte HG3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG3530, HG3540 oder HG3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden. |
| | FUNCTION | e | This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function. |

BCSU

The modules are configured in the system and activated with the AMO BCSU.



Configuration Management --> System Data --> Board --> Board
Click **New**, enter data (**IP Address**, section **IP Gateway, STMI Board Data** tab) and **Save**.



```
ADD-BCSU:MTYPE=IPGW,LTU=5,SLOT=91,PARTNO=Q2316-X,FCTID=1,FCTBLK=1,IPADDR=192.168.1.11,BCHL3570=40;
CHANGE-BCSU:TYPE=HWYBDL,LTU=5,SLOT=91,PARTNO=Q2316-X,HWYBDL=A;
```

NOTE: Prior to ADD-BCSU, use **ping** to check that the IP addresses given to you by the administrator are reachable.

IPADDR must not respond as this would indicate that the corresponding address has already been assigned.

IPADDR must be set differently for every board. The AMO does not verify if this rule is observed.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|------|-----------|----------------------|--|
| BCSU | BKAN3570 | d | Anzahl der B-Kanäle für die IPDA (HG3570) Funktion |
| | BCHL3570 | e | Amount of b-channels for IPDA (HG3570) function |
| | LTG | d | LTG-Nummer Parameter kann entfallen - oder muss auf 1 gesetzt werden. |
| | LTG | e | Line/Trunk Group Number Parameter can be omitted - or must be set to 1. |
| | LTU | d | LTU-Nummer des Rahmens, in dem die HG 3500 eingesetzt wird. Die HG 3500 darf nur in den Rahmen des HiPath 4000 Zentralsystems (LTU 1..15) eingesetzt werden. Der Rahmen muss mit einer LTUCX Baugruppe ausgestattet sein. |
| | LTU | e | Line/Trunk Unit Number of the shelf where the HG 3500 is plugged. An HG 3500 may only be used in a shelf of the HiPath 4000 central system (LTU 1..15). The shelf must be equipped with a LTUCX board. |
| | EBT | d | Einbauteilung des Steckplatzes der HG 3500 |
| | SLOT | e | Slot where the HG 3500 resides. |
| | SACHNR | d | Sachnummer der HG 3500-Baugruppe |
| | PARTNO | e | Part Number of the HG 3500 Board |
| | FCTID | d | Function ID |

Configuring the IPDA Feature

Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 System

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|------------|----------------------|---|
| | FCTID | e | Function ID |
| | LWVAR | d | LW Parametrisierung Wird für HG 3500 nicht benötigt. Wert sollte ausgelassen oder auf 0 gesetzt werden. |
| | LWVAR | e | LW Parametrization Not needed for HG 3500. Parameter should be omitted or set to 0. |
| | IPADR | d | IP-Adresse der HG 3500 Baugruppe Diese IP-Adresse muss zum HiPath 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Table “NETADR” on page 4-42) IPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. |
| | IPADDR | e | IP Address of the HG 3500 Board This IP address must belong to the HiPath 4000 LAN Segment (see NETADDR in AMO SIPCO, Table “NETADDR” on page 4-42) IPADDR must be different for every board. The AMO does not check compliance with this rule. |
| | HWYBDL | d | Highway Bündel Die HG 3500 / STMI2/4 Baugruppe unterstützt die Wideband Technologie. Deshalb muss der Baugruppe entweder das Highway Bündel A (default) oder F zugewiesen werden. |
| | HWYBDL | e | Highway Bundle The HG 3500 / STMI2/4 board supports wideband technology. Thus either highway bundle A (default) or F must be assigned to this board. |
| | TYPE=IPGW | d | Baugruppentyp IP Gateway = Common Gateway |
| | MTYPE=IPGW | e | board hardware type IP gateway = common GATEWAY |

4.4 Configuring Special Routes

The usual demands made on the routing between access points and HG 3500 modules in the central HiPath 4000 switch are fully met by the administration described above. A default router (AMO SIPCO, parameter **DEFRT**) serves the HiPath 3500 processors as an access to the IP world beyond the HiPath 4000 LAN segment. One default router per LAN segment in which access points are located serves the access points as a bridge to other network segments.

However, additional demands may be imposed by the specific network architecture of the customer.

A distinction is to be made between 2 basic scenarios in this context:

- Links between LAN segments containing access points which do not lead to the respective LAN segments via the default router.
- Links from the HiPath 4000 LAN segment to LAN segments containing access points which do not lead to the HiPath 4000 LAN segment via the default router.

The difference is that, in the first case, only HG 3575 routing tables are affected, while in the second case, the routing tables of all HG 3500 modules, as well as the CC computer and the UNIX part in the ADP, are also affected.

The routing tables of the HG 3500 and HG 3575 allow the configuration of 8 routes (in addition to default routes which do not appear in the routing table). These are configured by specifying a target (IP) address, the netmask of the target network and the IP address of the router port to be accessed by the source module.

It must be ensured that:

- no duplicate routes are entered, e.g.

| | | | | |
|---------------|---|---------------|---|--------------|
| 192.168.23.99 | , | 255.255.255.0 | , | 192.168.22.2 |
| 192.168.23.98 | , | 255.255.255.0 | , | 192.168.22.2 |

The first entry already leads the route into the entire network segment 192.168.23.X via the router port 192.168.22.2. The second entry would achieve precisely the same and, therefore, must be suppressed.

- the configuration of the route from A to B remains in place without influencing the route from B to A.

In other words, a route back to the source must generally also be configured in the target module, e.g.

| | | | | |
|---------------|---|---------------|---|--------------|
| 192.168.22.43 | , | 255.255.255.0 | , | 192.168.23.2 |
|---------------|---|---------------|---|--------------|

Configuring the IPDA Feature

Configuring Special Routes

4.4.1 Special Routes Between Access Points

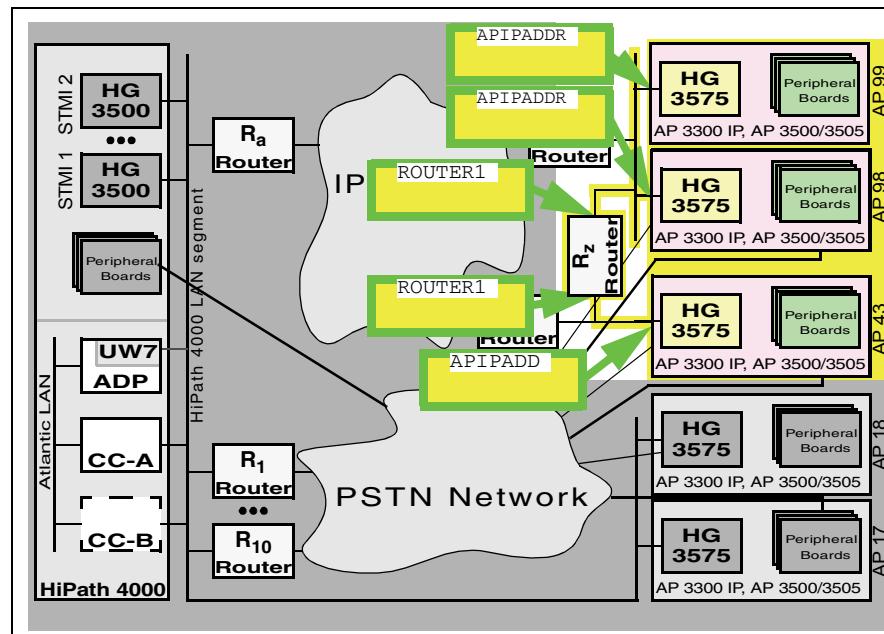


Figure 28 Special routes between access points

Generation

The configuration of special routes in HiPath HG 3575 (NCUI2/4S) is realized with the AMO APRT in the ROUTTBL branch.

Configuring the scenario illustrated in [Figure 28 “Special routes between access points”](#):



Configuration Management --> System Data --> IPDA --> HG3575 Additional Routing

Click **New** if there are no existing entries. Enter **LTU**.

Enter the IP addresses of the destinations and routers, enter the network masks in the routing table and **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=99,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.23.2;  
Sets the route from AP99 to AP43 via Router Rz.
```

```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=98,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.23.2;  
Sets the route from AP98 to AP43 via Router Rz.
```

```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43,  
DSTADDR1=192.168.23.99,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.22.2;  
Sets the route from AP43 to AP98 - and AP98 - via Router Rz.
```

In this example, the first of the 8 routing table entries was used in all 3 modules. Of course, this presupposes that these entries have not yet been used.

If the first 2 entries had already been used in AP43, the following would need to be done:



**Configuration Management --> System Data --> IPDA --> HG3575
Additional Routing**

Click **Search** and select **LTU**.

Enter the IP addresses in line 3 of the routing table and **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43,  
DSTADDR3=192.168.23.99,DSTMSK3=255.255.255.0,  
ROUTER3=192.168.22.2;
```

Table 13 “AMO APRT parameters in CHANGE branch under TYPE=ROUTTBL” on page 4-108 provides a precise description of the parameters.

If a **ROUTTBL** entry is to be deleted (e.g. the second entry in AP43), this is realized as follows:



**Configuration Management --> System Data --> IPDA --> HG3575
Additional Routing**

Click **Search** and select **LTU**.

Delete the IP addresses in the second line of the routing table and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



```
DELETE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43,INDEX=2;  
In order for these changes to become effective in the access point, this has  
to be restarted with
```

```
EXEC-USSU:MODE=UPDATAP,LTU=xx;
```

NOTE: Connections are cleared down without further warning.

Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk.

Configuring the IPDA Feature

Configuring Special Routes

4.4.2 Special Routes between Access Point and HiPath 4000 LAN Segment

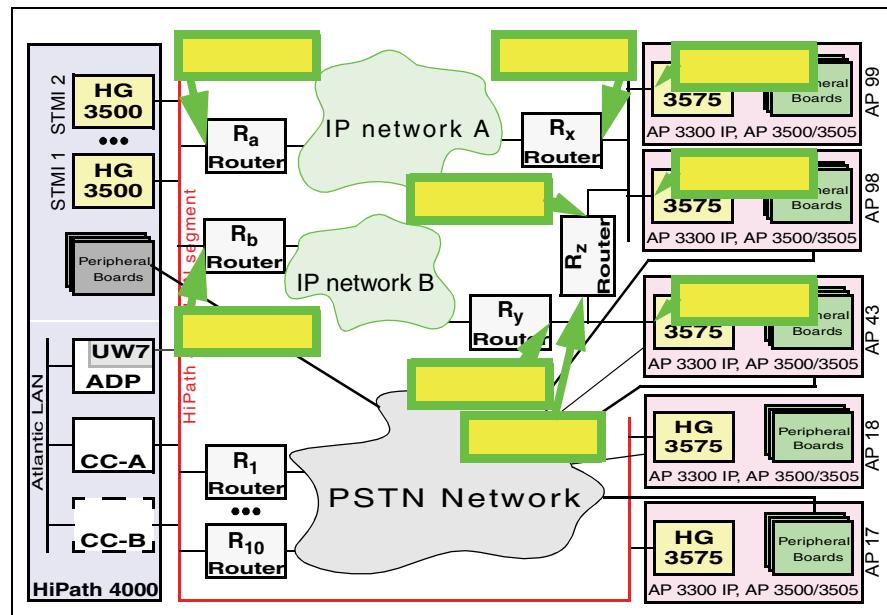


Figure 29 Special routes between access point and HiPath 4000 LAN segment

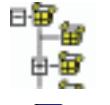
This complicated scenario is based on the simple case of the special route between 2 access points. In addition, the IP network of the customer in this case is broken down into 2 sub-networks which are not, or only, linked to one another via the HiPath 4000 LAN segment.

This scenario assumes that the routers a, x and y are the default routers (for HiPath 4000 components) in the respective networks.

Without additional routes, neither the HiPath HG 3500, nor the "direct link" access points AP17 and AP18 can reach access point AP 43.

The configuration for the entire scenario is realized according to the following steps:

- Configure Router R_a as the default router for all HG 3500 modules



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click Search and enter the default router address, then Save.



ADD-SIPCO: ... DEFRT=192.168.1.254 ...;

- Configure Router R_a as the default router for AP17 and AP18


Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Enter the router address on the **IP Interface (DL)** tab, then **Save**.



```
ADD-UCSU:UNIT=AP,LTU=17, ... APRTADDR=192.168.1.254  
...;  
and
```

```
ADD-UCSU:UNIT=AP,LTU=18, ... APRTADDR=192.168.1.254  
...;
```

- Configure Router R_x as the default router for AP98 and AP99 and specify Router R_a as the route for the signaling messages of the CC-A and CC-B, respectively


Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Enter the router addresses on the **IP Interface (NW)** tab, then **Save**.



```
CHANGE-UCSU:UNIT=AP,LTU=98, ...  
LSRTADDR=192.168.1.254,APRTADDR=192.168.23.1 ...;  
and
```

```
ADD-UCSU:UNIT=AP,LTU=99, ...  
LSRTADDR=192.168.1.254,APRTADDR=192.168.23.1 ...;
```

- Configure Router R_y as the default router for AP43 and specify Router R_b as the route for the signaling messages of the CC-A and CC-B, respectively


Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Enter the router addresses on the **IP Interface (NW)** tab, then **Save**.



```
ADD-UCSU:UNIT=AP,LTU=43, ...  
LSRTADDR=192.168.1.253,APRTADDR=192.168.22.1 ...;
```

The payload between AP43 and AP98/AP99 would now be routed via Router R_y -> Router R_b -> Router R_a -> Router R_x. The shortcut via Router R_z is configured as in the previous example with:

- Set the routes from AP43 to AP98/AP99 via Router R_z


Configuration Management --> System Data --> IPDA --> HG3575 Additional Routing

Click **Search**, select the access point, enter or change IP addresses, then click **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=43,  
DSTADDR1=192.168.23.99,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.22.2;
```

For the payload route from AP98/AP99 to AP43, special routes likewise have to be configured:

Configuring the IPDA Feature

Configuring Special Routes

- Set the routes from AP98/AP99 to AP43 via Router R_z



Configuration Management --> System Data --> IPDA --> HG3575 Additional Routing

Click **Search**, select the access point, enter or change IP addresses, then click **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=98,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.23.2;
```

```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=99,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.23.2;
```

The payload from the HG 3500 to AP98/AP99 is routed via the default router, R_a. The route is already specified with ADD-SIPCO.

The payload from AP98/AP99 to the HG 3500 is routed via the default router, R_x. The route is already specified with ADD-UCSU.

However, for the payload transport from the HG 3500 to AP43, the route is still missing. In this case, a special route has to be configured for all HG 3500s (STMI2/4) via Router R_b:

- Set the route from the HG 3500 to AP43 via Router R_b



Configuration Management --> System Data --> IPDA --> HG3570 Additional Routing

Click **Search**, enter or change network mask, destination and router addresses, then click **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=STMI,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.1.253;
```

The payload from AP43 to the HG 3500 is routed via the default router, R_y. The route is already specified with ADD-UCSU.

The payload between the HG 3500 and the “direct link” access points AP17/AP18 and back remains within the HiPath 4000 LAN segment and requires no additional routes.

The payload between the “direct link” access points AP17/AP18 and AP98/AP99 and back is routed via the route specified with ADD-UCSU. (R_a, R_x)

However, for the payload transport from the “direct link” access points AP17/AP18 and AP43, the route is still missing. In this case, a special route has to be configured via Router R_b:

- Set the routes from AP17/AP18 to AP43 via Router R_b

**Configuration Management --> System Data --> IPDA --> HG3575****Additional Routing**

Click **Search**, select the access point, enter or change network mask, destination and router addresses, then click **Save**.



```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=17,
```

```
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.1.253;
```

```
CHANGE-APRT:TYPE=ROUTTBL,MTYPE=NCUI,LTU=18,  
DSTADDR1=192.168.22.43,DSTMSK1=255.255.255.0,  
ROUTER1=192.168.1.253;
```

The payload from AP43 to AP17/AP18 is routed via the default router, R_y, and no additional routes need to be configured.

In order for these changes to become effective in the access points, these have to be restarted.

**Configuration Management --> System Data --> IPDA --> IPDA System Data**

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



```
EXEC-USSU:MODE=UPDATAP,LTU=xx;
```

NOTE: Connections are cleared down without further warning.

Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk.

In order for these changes to become effective in the HG 3500, **all** HiPath HG 3500 modules have to be restarted.

**Configuration Management --> System Data --> Maintenance --> Board Maintenance**

Click **Search** and select **STMI**.

Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.



```
RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X,FCTID=1;
```

NOTE: Connections are cleared down without further warning.

In order to maintain an overview in these somewhat more complex scenarios, the creation of a communications matrix is recommended:

Configuring the IPDA Feature

Configuring Special Routes

| from | to | CC-A | CC-B | HG 3500 | AP 17 | AP 18 | AP 43 | AP 98 | AP 99 |
|---------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| CC-A | - | - | - | - | direct | direct | R _b | R _a | R _a |
| CC-B | - | - | - | - | direct | direct | R _b | R _a | R _a |
| HG 3500 | - | - | - | - | direct | direct | R _b | R _a | R _a |
| AP 17 | direct | direct | direct | direct | - | direct | R _b | R _a | R _a |
| AP 18 | direct | direct | direct | direct | direct | - | R _b | R _a | R _a |
| AP 43 | R _y | - | R _z | R _z | R _z |
| AP 98 | R _x | R _z | - | direct | |
| AP 99 | R _x | R _z | direct | - | |

Table 12 Communication matrix for Figure 29

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|---|
| APRT | MTYP | d | <p>Modul Typ Hier wird zwischen STMI2/4 (HiPath HG 3500) und NCUI2/4 (HiPath HG 3575) unterschieden. MTYP=STMI: Diese Routing Table gilt für alle STMI2/4 im System gleichermaßen. DSTADR_x darf nicht zum HiPath 4000 LAN Segment gehören. ROUTER_x muss zum HiPath 4000 LAN Segment gehören. (siehe NETADR im AMO SIPCO, Table “NETADR” on page 4-42) MTYP=NCUI: Diese Routing Tabelle gilt nur für die durch LTU angegebene NCUI2/4. Bei Routen zwischen 2 NCUI2/4 müssen bei beiden NCUI2/4 die entsprechenden Einträge gemacht werden!</p> |

Table 13 AMO APRT parameters in CHANGE branch under TYPE=ROUTTBL

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | MTYPE | e | <p>Modul Type This is to distinguish between STMI2/4 (HiPath HG 3500) and NCUI2/4 (HiPath HG 3575).</p> <p>MTYPE=STMI: This routing table is common to all the STMIs in the system. DSTADDRx must not belong to the HiPath 4000 LAN Segment. ROUTERx must belong to the HiPath 4000 LAN Segment. (see NETADDR in AMO SIPCO, Table “NETADDR” on page 4-42)</p> <p>MTYPE=NCUI: This routing table is valid only for the NCUI2/4 assigned by LTU. For routes between 2 NCUI2/4 entries must be made for both NCUI2/4 respectively!</p> |
| | DSTADR1 | d | Zieladresse der 1. Route. Legt die Adresse fest, die über die im 1. Eintrag spezifizierte Route erreicht werden soll. Das kann eine Host- oder auch eine Netzadresse sein. Die DSTMSK1 erlaubt die Interpretation. |
| | DSTADDR1 | e | Destination Address for the 1st Route. Assigns the address to be reached using the route defined in the 1. entry. It may be a host or a network address. DSTMSK1 allows the interpretation. |
| | DSTMSK1 | d | Netzmaske des Netzes, dem DSTADR1 angehört |
| | DSTMSK1 | e | Netmask of the network which DSTADDR1 is part of |
| | ROUTER1 | d | IP-Adresse des Routers, über den Pakete an DSTADR1 gesendet werden sollen. Diese IP-Adresse muss zum HiPath 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Table “NETADR” on page 4-42) |
| | ROUTER1 | e | IP Address of the Router via which Packets to DSTADDR1 are to be sent. This IP address must belong to the HiPath 4000 LAN Segment (see NETADDR in AMO SIPCO, Table “NETADDR” on page 4-42) |
| | DSTADR2 | d | Zieladresse der 2. Route. |
| | DSTADDR2 | e | Destination Address for the 2nd Route. |
| | DSTMSK2 | d | Netzmaske des Netzes, dem DSTADR2 angehört |
| | DSTMSK2 | e | Netmask of the network which DSTADDR2 is part of |
| | ROUTER2 | d | IP-Adresse des Routers, über den Pakete an DSTADR2 gesendet werden sollen. |

Table 13

AMO APRT parameters in CHANGE branch under
TYPE=ROUTTBL

Configuring the IPDA Feature

Configuring Special Routes

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|---|
| | ROUTER2 | e | IP Address of the Router via which Packets to DSTADDR2 are to be sent. |
| | DSTADR3 | d | Zieladresse der 3. Route. |
| | DSTADDR3 | e | Destination Address for the 3rd Route. |
| | DSTMSK3 | d | Netzmaske des Netzes, dem DSTADR3 angehört |
| | DSTMSK3 | e | Netmask of the network which DSTADDR3 is part of |
| | ROUTER3 | d | IP-Adresse des Routers, über den Pakete an DSTADDR3 gesendet werden sollen. |
| | ROUTER3 | e | IP Address of the Router via which Packets to DSTADDR3 are to be sent. |
| | DSTADR4 | d | Zieladresse der 4. Route. |
| | DSTADDR4 | e | Destination Address for the 4th Route. |
| | DSTMSK4 | d | Netzmaske des Netzes, dem DSTADR4 angehört |
| | DSTMSK4 | e | Netmask of the network which DSTADDR4 is part of |
| | ROUTER4 | d | IP-Adresse des Routers, über den Pakete an DSTADDR4 gesendet werden sollen. |
| | ROUTER4 | e | IP Address of the Router via which Packets to DSTADDR4 are to be sent. |
| | DSTADR5 | d | Zieladresse der 5. Route. |
| | DSTADDR5 | e | Destination Address for the 5th Route. |
| | DSTMSK5 | d | Netzmaske des Netzes, dem DSTADR5 angehört |
| | DSTMSK5 | e | Netmask of the network which DSTADDR5 is part of |
| | ROUTER5 | d | IP-Adresse des Routers, über den Pakete an DSTADDR5 gesendet werden sollen. |
| | ROUTER5 | e | IP Address of the Router via which Packets to DSTADDR5 are to be sent. |
| | DSTADR6 | d | Zieladresse der 6. Route. |
| | DSTADDR6 | e | Destination Address for the 6thRoute. |
| | DSTMSK6 | d | Netzmaske des Netzes, dem DSTADR6 angehört |
| | DSTMSK6 | e | Netmask of the network which DSTADDR6 is part of |
| | ROUTER6 | d | IP-Adresse des Routers, über den Pakete an DSTADDR6 gesendet werden sollen. |
| | ROUTER6 | e | IP Address of the Router via which Packets to DSTADDR6 are to be sent. |
| | DSTADR7 | d | Zieladresse der 7. Route. |
| | DSTADDR7 | e | Destination Address for the 7th Route. |
| | DSTMSK7 | d | Netzmaske des Netzes, dem DSTADR7 angehört |
| | DSTMSK7 | e | Netmask of the network which DSTADDR7 is part of |

Table 13

AMO APRT parameters in CHANGE branch under
TYPE=ROUTTBL

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|-----|-----------|----------------------|--|
| | ROUTER7 | d | IP-Adresse des Routers, über den Pakete an DSTADR7 gesendet werden sollen. |
| | ROUTER7 | e | IP Address of the Router via which Packets to DSTADDR7 are to be sent. |
| | DSTADR8 | d | Zieladresse der 8. Route. |
| | DSTADDR8 | e | Destination Address for the 8th Route. |
| | DSTMSK8 | d | Netzmaske des Netzes, dem DSTADR8 angehört |
| | DSTMSK8 | e | Netmask of the network which DSTADDR8 is part of |
| | ROUTER8 | d | IP-Adresse des Routers, über den Pakete an DSTADR8 gesendet werden sollen. |
| | ROUTER8 | e | IP Address of the Router via which Packets to DSTADDR8 are to be sent. |

Table 13

AMO APRT parameters in CHANGE branch under
TYPE=ROUTTBL

4.5 Configuring Signaling Survivability

HiPath 4000 IPDA is an architecture with a central system and numerous “unintelligent” peripheral modules. An access point is essentially “remotely controlled” by the central system. If the control link fails, the access point cannot survive autonomously. It must forward signaling messages from the peripheral modules to the central system. It cannot process these itself. Therefore, in the event of a failure in the control link with the central system, the access point has no option other than to reset itself and wait until the central system restores it to operational status.

Thus, if the control link between the central system and an access point fails, the access point can no longer place telephone calls.

On account of these very severe consequences of a failure in the control link between the HiPath 4000 central system and the access point, a possibility of surviving such failures has been created. In the event of a fault, signaling survivability switches the control link from the IP network to an alternative route.

Calls possible with signaling survivability:

- Calls within the access point
 - Full scope of features
- Trunk calls from subscribers in the access point via local trunks
 - Full scope of features (for trunk calls)
- Calls with subscribers in other access points to which an IP connection can still be established for the payload
 - Full scope of features

Calls with subscribers in the central system and calls with subscribers in access points to which no IP connection can be established for the payload are only possible if the “Payload Survivability” feature is configured for the relevant components. However, even if “Payload Survivability” is configured, only “Basic Call” functionality can be guaranteed.

Please refer to [Section 4.8, “Configuring Payload Survivability”, on page 149](#).

Signaling survivability is sold as a performance feature and is configured individually for each access point.

4.5.1 How is the Fault Detected?

The control link (-> signaling link) between the CC and access point is a TCP connection. TCP connections are generally subject to permanent monitoring of their functionality. Transmitted packets are acknowledged. If the acknowledgement does not arrive within a certain time, the packet is repeated. If a packet cannot be delivered successfully within a specified duration, the sender receives a negative acknowledgement. Even if no packets are currently being transmitted, TCP checks that the connection is functional. To this end, so-called "Keep Alive" messages are sent at predetermined intervals, which have to be answered.

When a fault is reported on a signaling link, a relatively long period (e.g. more than 30 seconds) has already passed since the first indication). If it is assumed that signaling messages for a HiPath 4000 switch have to be delivered within a specified time (e.g. 60 seconds), the difference between these two times is available to find and establish an alternative route and re-transmit the messages.

The time can be shortened by drastically reducing the time between the error index and the message.

Therefore, a supervisory link is always established in HiPath 4000 between the CC and the access point parallel to the signaling link as soon as signaling survivability is configured for the access point.

This supervisory link is used exclusively to exchange "Keep Alive" messages at very short intervals (e.g. every second).

If the CC fails to receive a response to a "Keep Alive" message within a definable time interval (supervisory time), it switches the routing of the signaling messages to this access point from the IP router (e.g. R_a) to the survivability router (e.g. R₁).

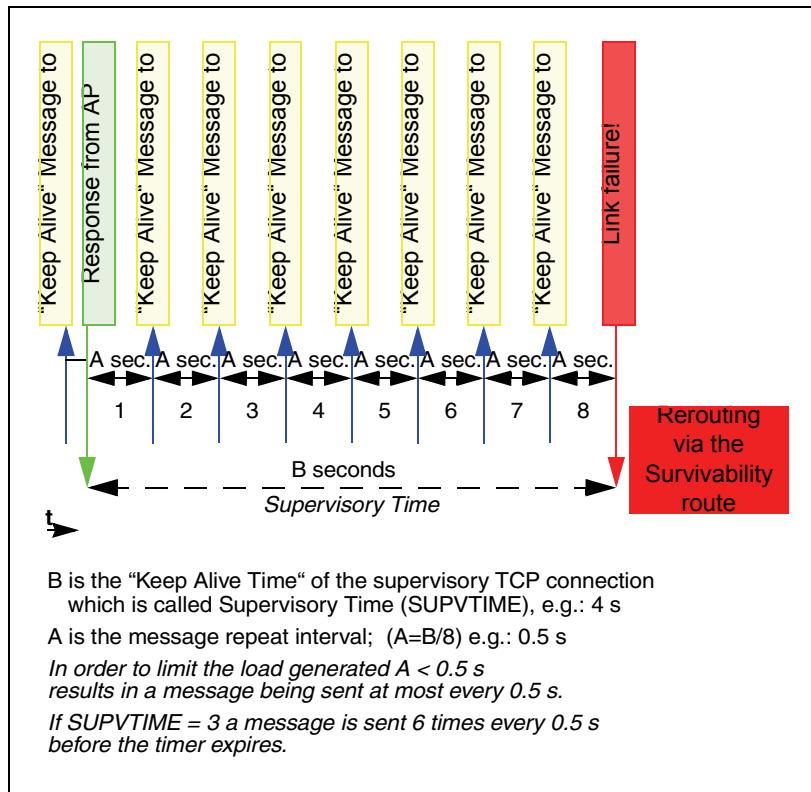


Figure 30 Supervisory message flow for signaling survivability in the CC

An escalation strategy is also triggered in the access point.

An interface fault is reported if, irrespective of the supervisory link, messages do not reach the access point on the signaling link within the set time interval (ALVTIME), either via the IP network or the alternative route.

After the interface fault report (ALVTIME) the access point is taken out of attendant list and will be reset within a definable time interval (RESTIME). It then waits for a renewed contact through the HiPath 4000 CC.

Up to end of ALVTIME, all signaling messages queued in the CC and in the access point for transmission are buffered. If the alive time (ALVTIME) expires, it can be assumed that the stored messages are outdated and may no longer be delivered. However, this means that the message flow between the CC and the access point is no longer consistent.

The time constants can be changed with the AMO SIPCO in the TIMING branch. (see [Section 4.1, "System timing \(TIMING\)", on page 48](#))

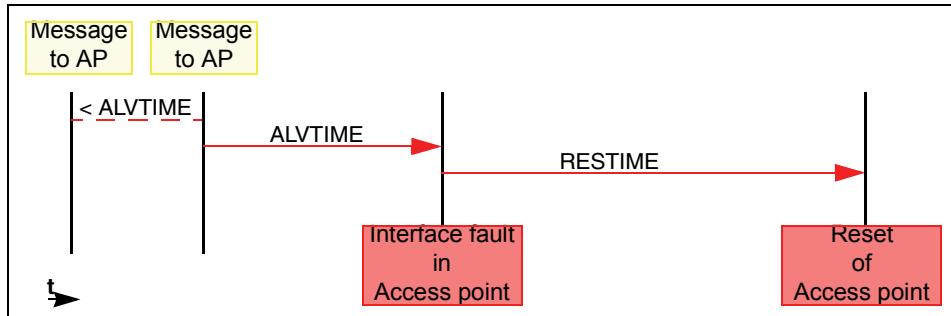


Figure 31 Message flow for signaling survivability in the access point

4.5.2 What is Used as an Alternative Route for Signaling?

If the IP link of an access point fails, an alternative route in a network is required that is not affected by the failure.

The basic demand on the network for the alternative route is simple:

- It must be independent of the IP network whose fault is to be bypassed via the alternative route.
- A connection device for the access point is required, which acts as a modem. It must be actively callable and provide the access point with “Ring Indication”.
- The central system must be supported by a corresponding router or an STMI2/4 with WAML function.

As a rule, an access point with signaling survivability generally requires a telephone connection for this purpose. The connection should be in the public PSTN network. Alternatively, it may be in a private network, insofar as the connection is not routed via the (IP) network whose fault is to be bypassed via the alternative route.

NOTE: The modem may **not** access the public network via the access point. It requires a separate connection independent of the access point.

If the LAN connection fails, the access point can no longer be controlled.

If the alternative route to the modem is routed via the access point, it cannot be switched before the alternative route is activated. However, it cannot be activated before being switched in the access point.

The access point is equipped with an RS 232/ V.24 interface on the HG 3575 module in order to connect a modem, via which the alternative signaling route into the telephone network is routed.

Configuring the IPDA Feature

Configuring Signaling Survivability

The counterpart to this modem is a special router at the HiPath 4000 LAN segment, referred to here as the survivability router. This router also requires access to the telephone network.

The transmission methods between the router and the modem must be compatible. Whenever possible, a digital link between the router and the modem should be used (ISDN modem), as analog modems require a long time to measure the route and agree on a transmission method. If the supervisory timer of the CC or access point expires during the link establishment time, there is a danger of messages being lost. The access point then resets itself. In addition, transmissions rates are substantially lower with analog modems than via ISDN. This can lead to delays with signaling messages and to the supervision timer expiring during bottleneck situations, in which case the access point resets itself in the end.

Approximately 64 Kbps are generally considered to be sufficient for the maximum transmission capacity required in the signaling path. The transmission rate offered by ISDN modems comes sufficiently close to this value. In the case of analog modems, at most half of the transmission bandwidth can be achieved. This can lead to the limitations described. A transmission bandwidth of at least 28.8 Kbps must be guaranteed. A path is considered unsuitable for survivability if a lower bit rate is used for modem connects due to low-quality links.

Depending on the connection capacity, a survivability router can operate up to 30 access points (router with S2 connection). As it cannot be foreseen precisely where in the IP network a fault will occur, the router capacity must be designed for the worst case scenario, i.e. failure of the link from the HiPath 4000 LAN segment to the IP network of the customer. In such a case, alternative signaling routes will be needed immediately for all access points with signaling survivability.

NOTE: If the modem connection goes over the public network, connection charges will accrue.

The link to an access point is used as long as the access point is not accessible via the IP network.

The configuration of the survivability router contains a setting for the period of "non-use" after which this link is disconnected. This "hold-time" does not form part of the HiPath 4000 IPDA configuration.

Accessibility of the access point via the modem connection is checked on a cyclical basis (RTO). The check can also be started directly using the AMO TSU. In these cases too, charges for the link will accrue in the PSTN.

NOTE: The connection from the active processor (CC-A or CC-B) to the survivability router runs via the HiPath 4000 LAN segment, just like the connection to the normal LAN router. If this LAN segment fails, for instance because a central L2 switch is faulty, the signaling survivability function will also fail. This "single point of failure" can be somewhat mitigated if CC-A and CC-B are connected to

different L2 switches and, for example, half the survivability routers and half the HG 3500 are each connected to the relevant switches. This ensures that at least half of the system will still be available should one of the two L2 switches fail.

4.5.3 Generation

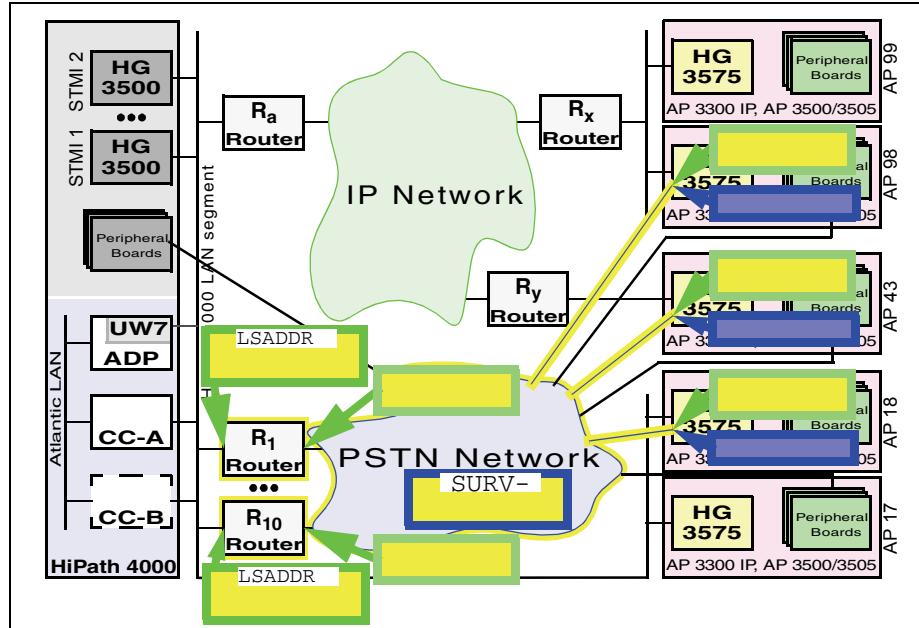


Figure 32 Configuring signaling survivability

The access connections of the survivability routers and modems into the PSTN telephone network form a virtual IP network, the survivability network. Every access to this virtual network requires an IP address in this network. In order to keep the administrative effort for this network to a minimum, a number of stipulations have been agreed on:

- The survivability network has the netmask 255.255.255.0.
- A maximum of 10 survivability routers are supported between the HiPath 4000 LAN segment and the survivability network; these are numbered consecutively from 1 to 10. The fourth digit in the IP address of routers in the survivability network is the consecutive number of the router, i.e. 1-10.
- The address of an access point in the survivability network is likewise specified. The fourth section of the IP address is set to be identical to the LTU number of the access point.

Thus, only one parameter essentially remains to be configured in the survivability network: the network address.

Configuring the IPDA Feature

Configuring Signaling Survivability

This is configured with the AMO SIPCO and must already be specified during ADD-SIPCO if the customer has purchased signaling survivability licenses (see Section 4.1, “Configuring the HiPath 4000 LAN Segment”).

If the licenses for signaling survivability are not purchased until later or if the zero address 0.0.0.0 was specified during initial installation, this address must be set now.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, enter or change the survivability network address on the **System Data** tab, then **Save**.



CHANGE-SIPCO:TYPE=LSNET, SURVNET=192.168.15.0;

NOTE: The last digit of the SURVNET address must always be ZERO. Otherwise, it would not be a network address, together with the specified netmask 255.255.255.0.

The licenses for signaling survivability can be queried as follows:



Configuration Management --> HiPath Inventory Management

--> HIM System Data --> Feature --> Marketing Units

Click **Search** --> **Sales Features** tab --> **Signaling Survivability** entry

DISP-CODEW; “SIGNALING SURVIVABILITY” entry

Although this network is only used when needed and the communication partners are fixed, the address for this network must be agreed on with the customer network administrator.

Thought now has to be given to the assignment of access points to survivability routers. Every survivability router can be described through the following data, which must also be configured in the router itself:

- Consecutive number of the router [1..10]
- IP address of the router in the HiPath 4000 LAN segment
- IP address of the router in the survivability network
- Access points to be operated via this router, including:
 - LTU number and, derived from that number, its IP address for survivability
 - Telephone number of the modem connection

Ultimately, the router is to be configured in such a way that, upon receipt of a packet with a target address identical to that of the survivability address of an access point, it establishes a dial-up connection to the modem of that access

point and subsequently transmits the packet. If the connection is not used for an extended period (e.g. 30 seconds), the access point can be reached again via LAN and the link to the modem can be disconnected.

An STM2/4 module with WAML function in the HiPath 4000 CC can also be used as a survivability router.

NOTE: If a survivability router is to access the ISDN network via the HiPath 4000, there must be sufficient connection capacity in the trunk access of the HiPath 4000.

If, for example, 83 access points on a system are equipped with signaling survivability, 83 B-channels to the CO must be made available immediately in the central area around the HiPath 4000 system in the event of an IP network failure. If this capacity is not reserved, it may not be possible to reach all access points. Access points that are not reached via signaling survivability perform a restart and can only operate again if they are accessed by CC via LAN or modem.

The configuration in the HiPath 4000 switch is realized as follows:

- Announce the survivability routers in the system



Configuration Management --> System Data --> IPDA --> IPDA Signaling Survivability Router

Click **Search**, enter or change the router number and address on the Router Data tab, then **Save**.



ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,

LSADDR=192.168.1.101;

ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10,

LSADDR=192.168.1.110;

Routers 1 and 10 from the example in [Figure 32 “Configuring signaling survivability”](#) are thus configured.

- Assign the access points to the survivability routers



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search**, set the desired router number on the **General** tab under signaling survivability and **Save**.



ADD-APRT:TYPE=SURV,CONF=AP,LTU=98,ROUTERNO=1;

ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=1;

ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=1;

Thus, all access points with signaling survivability in the example in [Figure 32 “Configuring signaling survivability”](#) are assigned to a router. Finally, when assigning the access points to a router, signaling survivability for the respective access point is configured. This command checks whether a license for signaling survivability is available. If so, the use is booked; if not, the configuration is rejected.

Configuring the IPDA Feature

Configuring Signaling Survivability

If the assignment of an AP to a survivability router is changed, e.g. if AP 43 should in future be operated by Router 10 instead of Router 1, the following action is required:



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search**, set the desired router number on the **General** tab under signaling survivability and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



A CHANGE of the configuration for signaling survivability with APRT is not possible. In order to change the configuration, the corresponding assignment is simply deleted and subsequently re-configured.

`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`

`ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=10;`
In order for this change to become effective, AP 43 has to be restarted.

`EXEC-USSU:MODE=UPDATAP,LTU=43;`

NOTE: Connections are cleared down without further warning.

Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|------|-----------|----------------------|---|
| APRT | ROUTERNR | d | Nummer des Routers für Signaling Survivability. HiPath 4000 IPDA unterstützt bis zu 10 Survivability Router, welche von 1..10 durchnummert und über diesen Index verwaltet werden. |
| | ROUTERNO | e | Number of the Router for Signaling Survivability. HiPath 4000 IPDA supports up to 10 survivability routers, numbered 1..10 which are administered using this index. |
| | LSADR | d | IP-Adresse eines Routers für Signaling Survivability im HiPath 4000 LAN Segment. Diese IP-Adresse muss zum HiPath 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Table “NETADR” on page 4-42) |

Table 14

AMO APRT parameters in ADD branch under TYPE=SURV,
CONF=ROUTER

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|--|
| | LSADDR | e | IP Address of a Router for Signaling Survivability in the HiPath 4000 LAN Segment. This IP address must belong to the HiPath 4000 LAN Segment (see NETADDR in AMO SIPCO, Table “NETADDR” on page 4-42) |

Table 14

AMO APRT parameters in ADD branch under TYPE=SURV,
CONF=ROUTER

| AMO | Parameter | Sprache/ Language | Beschreibung/Description |
|------|-----------|----------------------|---|
| APRT | ROUTERNR | d | Nummer des Routers für Signaling Survivability. Bestimmt einen der bis zu 10 Survivability Router, über den dieser Access Point erreicht werden soll. |
| | ROUTERNR | e | Number of the Router for Signaling Survivability. Selects one of the up to 10 survivability routers, via which this Access Point shall be reached. |

Table 15

AMO APRT parameters in ADD branch under TYPE=SURV,
CONF=AP

4.5.4 Is Signaling Survivability Currently Active? (DIS-UCSU)

When a system is operating with signaling survivability, it is often necessary - without analyzing any error messages - to query whether an access point is currently being controlled normally via LAN or whether it is being controlled via modem with signaling survivability.

This query is executed with the AMO UCSU.



The query with the AMO UCSU can only be executed in expert mode.
Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO
(see AMO command)



DISPLAY-UCSU:AP,1,;
The AMO returns an overview of all configured access points, containing not just configured parameters, but also current operating states.

| ADDRESS | TARGET CONFIG | STATUS | LTUC BOARD | LTU TYPE | FRMTYPE |
|--|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| | | | | | |
| CONNTYPE | LOCID | LOCATION | | | SRCGRP |
| PHONE: | | | FAX: | | |
| LSRTADDR | APRTADDR | | BCHLCNT | PLCHECK | SIGNAL. |
| +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ |
| AP 1.17 CONFIGURED | READY | Q2302-X10 | INCH19 | INCH19 | |
| | | | | | |
| APDL 001 MCH MACHTLFINGERSTR.1 CDR. 7202-111 | | | | | 1 |
| PHONE: 08972223456 | | FAX: 08972265432 | | | |
| 192.168.001.017 | 192.168.001.254 | 30 | YES | LAN | |
| +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ |
| AP 1.18 CONFIGURED | READY | Q2302-X10 | INCH19 | INCH19 | |
| | | | | | |
| APDL 001 MCH MACHTLFINGERSTR.1 CDR. 7202-111 | | | | | 1 |
| PHONE: 08972223456 | | FAX: 08972265432 | | | |
| 192.168.001.018 | 192.168.001.254 | 30 | YES | LAN | |
| +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ | +-----+-----+-----+-----+-----+ |
| AP 1.43 CONFIGURED | READY | Q2302-X10 | INCH19 | INCH19 | |
| | | | | | |

Figure 33

UCSU query (in the event of the failure of Router Rx)

4.5.5 Configuring the Modem

In order to be able to make the configuration settings, the modem must be connected to a PC and a terminal emulation program (HyperTerminal) must be started on the PC.

NOTE: The **Pocket ISDN TA** modem from *INSYS Microelectronics, S30122-X7551-X AYA422* is recommended for use as an IPDA survivability modem with ISDN interface.

The following must be set if they were not already set by default:

- The baud rate at the modem's serial interface must be set to 115200 bauds which is mostly covered via the auto-detect mode.
Modems that do not support the 115200 baud rate at the serial interface are unsuitable for use with IPDA.
- Auto-Answer must be switched **off**.
- The local echo must be switched **off**.
- The modem response to commands must be shown in plain text (in long form), i.e. as text "RING", "CONNECT", etc.
- Neither error correction nor compression must be activated in the modem. This is performed by the PPP itself.
- The software handshake (XON/XOFF) must be deactivated.
- *For ISDN modems:* the B-channel protocol: HDLC - PPP protocol ("async to sync" conversion, asynchronous PPP, single link PPP)
- *For analog modems:* set the line bit rate permanently on both modems to save negotiation time.

In response to the modem's "RING" message, the HG 3575 sends the "AT A" command to the modem which must report "CONNECT" within 60 seconds.

First the factory defaults must be restored

AT&F 

The parameters specified above must then be set

For modem **Pocket ISDN TA**

- Auto-Answer must be switched off:
ATS0=0 

- The local echo must be switched off:
ATE  or generally ATE0 

Configuring the IPDA Feature
Configuring Signaling Survivability

Finally, the configuration has to be saved:



4.5.6 Configuring the Router

4.5.6.1 Signaling Flow Survivability for “Networked“ Access Points

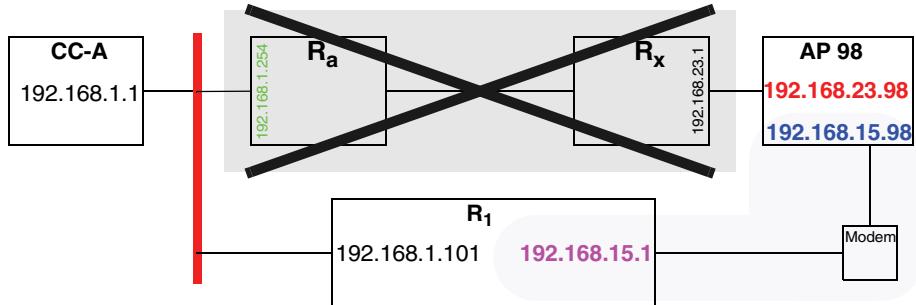


Figure 34

Survivability router configuration

The following process must be taken into consideration when configuring the survivability router.

Normal operation (without survivability):

CC-A generates packet at AP 98 with destination **192.168.23.98** and source 192.168.1.1 and transfers it to the R_a router (**192.168.1.254**).

This may send the packet via another router to R_x which delivers the packet to AP 98.

Survivability:

CC-A generates packet at AP 98 with destination **192.168.23.98** and source 192.168.1.1 and transfers it to the router R₁ under 192.168.1.101.

NOTE: The complete **IP frame**, including addresses, remains identical to the frame in normal operation.

With survivability, only the accessed router changes (in the HiPath 4000 LAN segment). This change takes the form of a different destination address at Ethernet level (MAC-DA).

The IP address of Router R₁ in the HiPath 4000 LAN segment is not accessed visibly. It is needed to determine the MAC address of the router port with ARP.

R₁ sends the packet to the next hop router **192.168.15.98** and creates the modem link for the PPP connection between **192.168.15.1** and **192.168.15.98** or uses the existing connection.

The packet is sent from the PPP instance **192.168.15.98** to the destination **192.168.23.98** in AP 98.

Configuring the IPDA Feature

Configuring Signaling Survivability

For this, the route for **192.168.23.98** must be configured via **192.168.15.98** in the survivability router R₁ and the dial-up connection for the destination **192.168.15.98**.

The PPP instance in R₁ must be configured with the address **192.168.15.1** so that packets from AP 98 can be transported back to CC-A.

4.5.6.2 Signaling Flow Survivability for “Direct Link“ Access Points

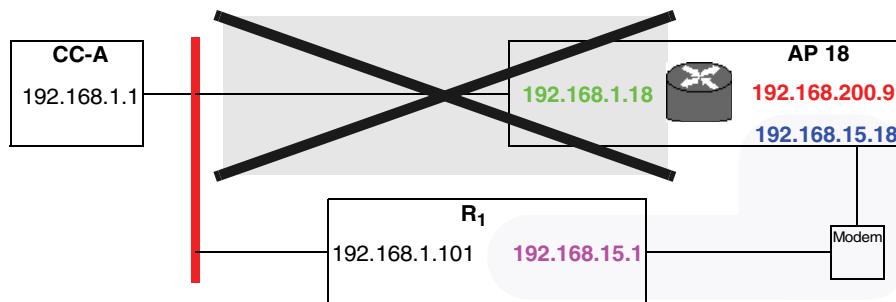


Figure 35 *Survivability router configuration*

The following process must be taken into consideration when configuring the survivability router.

Normal operation (without survivability):

CC-A generates packet at signaling unit AP 18 with destination **192.168.200.9** and source **192.168.1.1** and transfers it to the internal signaling router associated with AP 18 (**192.168.1.18**).

This sends the packet to the signaling unit AP 18 (**192.168.200.9**).

Survivability:

CC-A generates packet at AP 18 with destination **192.168.200.9** and source **192.168.1.1** and transfers it to the router R₁ under **192.168.1.101**.

NOTE: The complete **IP frame**, including addresses, remains identical to the frame in normal operation.

With survivability, only the accessed router changes (in the HiPath 4000 LAN segment). This change takes the form of a different destination address at Ethernet level (MAC-DA).

The IP address of Router R₁ in the HiPath 4000 LAN segment is not accessed visibly. It is needed to determine the MAC address of the router port with ARP.

R₁ sends the packet to the next hop router 192.168.15.18 and creates the modem link for the PPP connection between 192.168.15.1 and 192.168.15.18 or uses the existing connection.

The packet is sent from the PPP instance 192.168.15.18 to the destination 192.168.200.9 in AP 98.

For this, the route for 192.168.200.9 must be configured via 192.168.15.18 in the survivability router R1 and the dial-up connection for the destination 192.168.15.18.

The PPP instance in R₁ must be configured with the address 192.168.15.1 so that packets from AP 18 can be transported back to CC-A.

4.5.6.3 Signaling Survivability with WAML Replacement

WAML boards are no longer supported as of HiPath 4000 V4. However, the feature "Signaling Survivability with WAML Replacement" has been available since HiPath 4000 V2.0. Here, an STMI was configured with the WAML function (AMO BCSU, FCTID=5). The common gateway has been introduced as of HiPath 4000 V4. This must now be configured in the AMO BFDAT using the function =WAML. Either a separate board or a board that supports multiple functions can be used for this purpose.

NOTE: If this feature is configured (STMI board with WAML function), then the redundant LAN interfaces function does not work. See also [Section 10.5, "Redundant LAN Interface"](#).

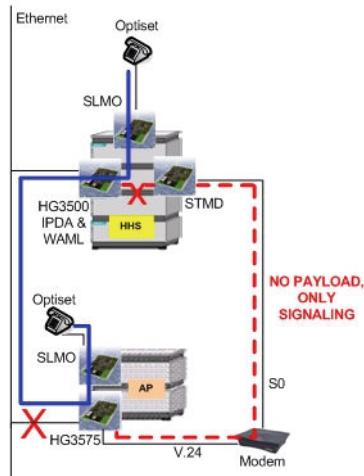


Figure 36 *Signaling survivability with WAML replacement*

HiPath 4000 configuration

For HiPath 4000 configuration please refer to "HG 3500 V4 - Serviceability / WAML Replacement", [Section 3.1, "Configuring the HiPath 4000"](#).

WAML configuration with WBM

- Router call number

Explorers -> Routing -> PSTN

The **PSTN Global Data** screen with the **Router Call Number** as configured in AMO LDPLN is displayed.

- PSTN

Explorers -> Routing -> PSTN Peers

The PSTN partner (**IP Address of PSTN Peer**) is the survivability-modem with its IP-Address coming from AMO SIPCO, parameter **SURVNET** + AP number, here **192.168.15.18** or **192.168.15.98**.

The PSTN interface (**IP Address of Local PSTN Interface**) is the PPP side of the STMI2/4 board with WAML function, that is, the AMO SIPCO, parameter **SURVNET** + router number, in this scenario **192.168.15.1**.

- PSTN Station Number

Explorers -> Routing -> PSTN Partner

The STMI2/4 board with the WAML function reaches the survivability modem with this station number. The station number is configured in the STMD with the **AMO SBCSU** and the parameter **STNO**; in the current scenario, this is **07123456** for AP 18 and **00303217654** for AP 98.

- Static Route

Explorers -> Routing -> IP Routing -> Static Routes

The destination (**Destination Network/Host**) is the signaling IP address in HG 3575 (NCUI2+/4) which is configured with the parameter **APIPADD** in the **AMO APRT** (IP address of AP 18 or AP 98).

The **Route Gateway** is the ISDN IP address of the modem (**AMO SIPCO**, parameter **SURVNET** + AP number): **192.168.15.18** or **192.168.15.98**

4.5.6.4 External ISDN Router as the Survivability Router

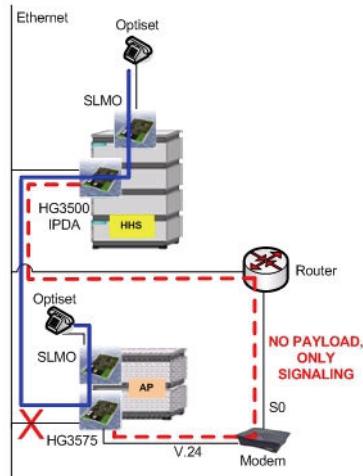


Figure 37 Signaling survivability without WAML replacement but with a router
By way of example, the settings for an external Cisco 1603R router are displayed.

NOTE: The setting for this router is merely provided as an example and is only intended to illustrate how to use the parameters in a router configuration. The router selected in this case is not a special recommendation and its availability cannot be guaranteed. Routers from other product lines and manufacturers can also be used.

Example Cisco 1603R

```

hostname srt-isdn1
!
ip subnet-zero
no ip finger
no ip domain-lookup
isdn switch-type basic-net3
file prompt quiet
!
interface Ethernet0
  ip address 192.168.1.101 255.255.255.0
  no ip directed-broadcast
!
interface BRI0
  ip address 192.168.15.1 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 192.168.15.43 name AP43 broadcast 00697654321
  dialer map ip 192.168.15.98 name AP98 broadcast 00303217654
  dialer map ip 192.168.15.18 name AP18 broadcast 07123456
  dialer-group 1
    isdn switch-type basic-net3
!
ip classless
ip route 192.168.22.43 255.255.255.255 192.168.15.43
ip route 192.168.23.98 255.255.255.255 192.168.15.98
ip route 192.168.200.18 255.255.255.255 192.168.15.18
!
dialer-list 1 protocol ip permit

```

APRT
TYPE=SURV
LSADDR

SIPCO
TYPE=LSNET
NETMASK

APRT
TYPE=SURV
ROUTERNO

SIPCO
TYPE=LSNET
SURVNET

Phone number that must be dialed in order to access the survivability modem

LTU number of AP

APRT
TYPE=APNET
APIPADDR

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

4.6 Configuring Quality Monitoring for the Signaling Connection over IP

As already described in [Section 4.5, “Configuring Signaling Survability”, on page 112](#), you cannot operate an access point unless the signaling connection is working properly.

The concept introduced with HiPath 4000 version 1.0 for monitoring the signaling connection uses the additional monitoring connection to verify if communication is basically possible between CC and an access point. The main advantage of this is that you can respond very quickly and activate signaling survivability in the event of a crash on the IP connection between CC and the access point.

The IP connection between the CC and access point is sometimes not completely severed, “just” severely restricted. This can have an extremely negative impact on the signaling function without this malfunction being detected by the separate monitoring connection.

To eliminate this restriction, we have introduced a new mechanism for monitoring the actual signaling connection to complement the mechanism already described and based on a separate monitoring connection.

This additional functionality is split into five components:

- [Restriction of the Available Signaling Bandwidth \(Traffic Shaping\)](#)
- [Monitoring the Runtime for Signaling Messages \(Round Trip Delay\)](#)
- [Monitoring Message Throughput](#)
- [Advanced Criteria for Signaling Survability](#)
- [Output of Statistical Information on the Signaling Connection](#)

4.6.1 Restriction of the Available Signaling Bandwidth (Traffic Shaping)

The signaling bandwidth for controlling an access points is not particularly large and fluctuates very heavily. A flat rate of 64 Kbps is required for the signaling connection, although in some configurations the minimum value of 32 Kbps is sufficient.

Bandwidth requirements spike briefly when a call processing action triggers numerous parallel follow-up actions in the peripherals. Several large packets containing signaling information can be sent to an access point in a short period of time. For a WAN router with a very low available bandwidth for this signaling connection (for example, 32 Kbps), this means that while the first packet from this burst is being sent, another is being received. The router may not have enough buffer space to buffer the packets. As a result, packets from this “burst” are rejected by the router and have to be resent later by the CC.

Restricting the signaling bandwidth to an access point in the CC prevents a burst from occurring when packets are immediately sent one after the other from the CC. This is done by staggering the packets so that they are sent at intervals that prevent buffer overflow in the router.

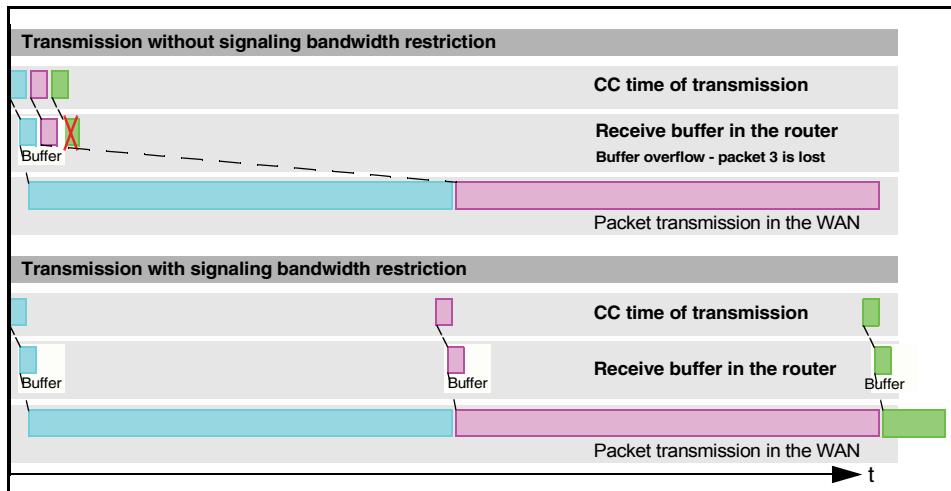


Figure 38 Signaling connection with/without bandwidth restriction

NOTE: If there is only a bandwidth of between 32 and 63 Kbps available for signaling to an access point in the IP network, then signaling bandwidth restriction **must** be activated in the CC and set to the value available in the network.

The signaling bandwidth restriction delays signaling messages in the CC and sometimes results in a backlog of several messages. If a backlog of this kind persists for several seconds, the signaling bandwidth configured is too low. The system issues the error message F8292 (see [Table 15 “F8292 - Bandwidth Requirement Exceeds Limit” on page 4-144](#)) that marks the beginning of backlog. The publication of a message status can also be a criteria for changing from the signaling path to the signaling survivability path (see [Section 4.6.4, “Advanced Criteria for Signaling Survivability”, on page 137](#)).

The message F8293 is output to signal that the backlog has cleared (see [Section 4.6.6.6, “F8293 - Bandwidth Required Back Below Limit”, on page 144](#)).

The restriction of the signaling bandwidth only affects the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

NOTE: Under-dimensioning the signaling bandwidth can lead to a message buffer deficit which results in a access point reset. All connections are then cleared down.

The system outputs the error message F8292 as soon as under-dimensioning is detected during live operation (see [Section 4.6.6.5, “F8292 - Bandwidth Requirement Exceeds Limit”, on page 144](#)). The signaling bandwidth **must** be

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

increased in response to this message. This applies both to the restriction in the system **and** the actual bandwidth available in the network. Ignoring these early warning signals can result in the access point reset described.

Procedure

At the start of each second, a transmission credit with the value of the signaling bandwidth configured is made available for use. If the setting is 40 Kbps, for example, 5000 bytes may be transmitted every second. For every packet to be sent, the credit is now reduced by the packet size. If there is not enough credit left, the packet is delayed until sufficient credit is available.

When the second expires, the remaining transmission credit is cancelled. The next second then starts again with a new credit for the value of the signaling bandwidth configured, for example, 5000 bytes. Returned packets can now be sent.

The transmission bandwidth is restricted at “application level“, in other words, over the TCP/IP stack.

Generation



Configuration Management --> System Data --> IPDA --> Access point
Click **Search** and enter or change the bandwidth on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.

CHANGE-STMIB:MTYPE=NCUI2, TYPE=SIGQOS, LTU=99, BANDW=40;

The signaling bandwidth is expressed in kilobits per second (Kbps). The value **BANDW=0** disables signaling bandwidth restriction. The setting becomes effective immediately.

4.6.2 Monitoring the Runtime for Signaling Messages (Round Trip Delay)

If a malfunction occurs in the IP network, the effective bandwidth available drops and the time between the dispatch of a message and receipt acknowledgement rises.

A maximum permissible message runtime can be defined for the signaling connection for every access point. This runtime includes the entire time from sending the message to receiving the acknowledgement, in other words, the “Round Trip Delay“. The runtime is evaluated with every signaling message. Measurement is therefore independent of the signaling load.

If the runtime exceeds the limit set, the system outputs the error message F8290 (see [Section 4.6.6.2, “F8290 - Net Weakness Start Message Runtime Exceeded”, on page 142](#)). The exceeding of the maximum message runtime can also be a criteria for changing from the signaling path to the signaling survivability path (see [Section 4.6.4, “Advanced Criteria for Signaling Survivability”, on page 137](#)).

The message F8291 is output to signal a return by the runtime to permitted values (see [Section 4.6.6.4, “F8291 - Net Weakness End”, on page 143](#)).

Monitoring the maximum message runtime is only active on the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

Procedure

An average runtime value is calculated and stored every three seconds for all messages acknowledged in this interval.

The three-second average values are used to generate further average values over a short (15 seconds: SHORT) and long monitoring time (60 seconds: LONG).

The error message is generated whenever either of the two values (SHORT/LONG) exceeds the limit configured.

The limit is set for the long monitoring duration (LONG). The limit for the short duration (SHORT) is set to factor 1.5 times the value.

The SHORT interval makes sense with a higher limit because if the network quality jumps, the system can respond faster, that is, within 15 seconds. This interval would be 60 seconds in the case of exact measurement.

The measurement is made at “application level”, in other words, over the TCP/IP stack. On account of stack dynamics, measured values cannot be compared directly with values that are measured directly on the network.

The runtime includes:

- Sender of packet from TCP level in the HiPath 4000 central system
- Transmission of packet in the network
- Receipt of packet on HG 3575 up to TCP
- Creation and sending of acknowledgement on the HG 3575
- Transmission of acknowledgement in the network
- Receipt of acknowledgement in the HiPath 4000 central system

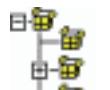
Since TCP can delay the acknowledgement of a packet in order to combine the acknowledgement with that of another packet, values under 400 ms are impractical.

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

Keep alive packets are not included in the measurement. If no packets are sent or acknowledged within a 3-second interval, a long-term mean value is used that is determined by the TCP.

Generation



Configuration Management --> System Data --> IPDA --> Access point
Click **Search** and enter or change the maximum runtime on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.



CHA-STMIB: MTYPE=NCUI2, TYPE=SIGQOS, LTU=99, MAXRTD=500;

The message runtime is expressed here in milliseconds. The value MAXRTD=0 disables message runtime monitoring. The setting becomes effective immediately.

NOTE: Measurements are performed at 10-ms intervals. As a result, it only makes sense to set values divisible by 10 (without remainder), for example, 400, 410, 420, etc.

4.6.3 Monitoring Message Throughput

A minimum necessary message throughput can be defined for the signaling connection for every access point. The throughput measurement includes the volume of all messages sent by the CC.

The undershooting of the minimum necessary message throughput only takes account of the times when the specified load at least was used. An undershooting of the minimum message throughput is ignored because the number of messages available for transmission is not sufficient.

If the throughput falls short of the threshold value set, the system outputs the error message F8290 (see [Section 4.6.6.3, “F8290 - Net Weakness Start Message Throughput Undershoot”, on page 143](#)). The undershooting of the minimum message throughput can also be a criteria for changing from the signaling path to the signaling survivability path (see [Section 4.6.4, “Advanced Criteria for Signaling Survivability”, on page 137](#)).

The message F8291 is output to signal a return by the message throughput to permitted values (see [Section 4.6.6.4, “F8291 - Net Weakness End”, on page 143](#)).

Monitoring the minimum message throughput is only active on the signaling path over LAN. The modem connection is not affected in the case of signaling survivability.

Procedure

Every three seconds the system calculates the number of bytes sent during this interval. The result is then used to calculate the throughput in Kbps. (*Bytes sent * 8/3*)

The three-second values are used to generate average values over a short (15 seconds: SHORT) and long monitoring time (60 seconds: LONG).

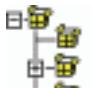
The error message is generated whenever either of the two values (SHORT/LONG) exceeds the limit configured.

The limit is set for the long monitoring duration (LONG). The limit for the short duration (SHORT) is set to 2/3 of the LONG value.

The SHORT interval makes sense with a lower limit because if the network quality jumps, the system can respond faster, that is, within 15 seconds. This interval would be 60 seconds in the case of exact measurement.

The measurement is made at “application level”, in other words, over the TCP/IP stack. On account of stack dynamics, measured values cannot be compared directly with values that are measured directly on the network.

Generation



Configuration Management --> System Data --> IPDA --> Access point
Click **Search** and enter or change the minimum message throughput on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.



CHA-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,MINTHRPT=32;

The minimum message throughput is expressed here in Kbps. The value MINTHRPT=0 disables message throughput monitoring. The setting becomes effective immediately.

4.6.4 Advanced Criteria for Signaling Survability

The restriction and monitoring functions described in [Section 4.6.1, “Restriction of the Available Signaling Bandwidth \(Traffic Shaping\)”](#) to [Section 4.6.3, “Monitoring Message Throughput”](#) can trigger the signaling path switchover from LAN to modem.

The events that should activate signaling survivability ([Section 4.5, “Configuring Signaling Survability”, on page 112](#)) are set for each access point in the course of configuration.

The following options are available:

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

- Switching over the signaling path to modem in the event of loss of monitoring connection (as described in [Section 4.5, “Configuring Signaling Survability”](#) - behavior of HiPath 4000 version 1.0) - [STD]
In STandard mode, the signaling path is switched back to LAN as soon as stability returns to the monitoring connection.
- Switching over the signaling path to modem in the event of loss of the monitoring connection or violation of the criteria from monitoring the quality of the signaling connection - [EXTENDED]
In EXTENDED mode, the signaling path is switched back to LAN as soon as stability returns to the monitoring connection and the quality criteria are satisfied. To measure the quality criteria, a load is periodically generated on the monitoring connection which must at least be able to transport the signaling connection after reverting to LAN.

NOTE: When using EXTENDED mode, the bandwidth available must be taken into consideration on the signaling path over modem. There is no point in switching to a 28.8-Kbps modem connection because the minimum throughput for the LAN connection falls short of 64 Kbps.

- Exclusive use of the signaling path on modem - [SURVONLY]
SURVONLY mode permits the administrative switchover of the signaling path to modem irrespective of behavior on the LAN connection. This can be used for stable switchover when performing planned maintenance in the LAN/WAN environment for the duration of the maintenance work. Switching back is then performed in STandard or EXTENDED mode

NOTE: Even in the case of administrative activation of signaling survivability for an access point, the establishment of new payload connections is blocked in the HiPath 4000 CC (to all HG 3500s).

Generation



Configuration Management --> System Data --> IPDA --> Access point
Click **Search** and select the switchover mode for signaling survivability on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.



CHA-
STMIB:MTYPE=NCUI2, TYPE=SIGQOS, LTU=99, SIGPTHSW=EXTENDED;

The setting becomes effective immediately.

4.6.5 Output of Statistical Information on the Signaling Connection

If monitoring is active for the message runtime or the message throughput, the system only signals the results of measurements if limits are breached.

It is therefore very difficult to say if the limits configured were set too low or even much too high.

For this reason, the cyclical output of measurement data can be set at the operating terminal.

You can set whether or not measurement data should be output cyclically for every access point.

Data is only output, however, if

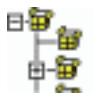
- monitoring is active for the message runtime or the message throughput
- output is generally enabled with the AMO-DIAGS (CC/HSR option S00)

The measurement data are output with the message F8289

NOTE: The cyclical query and output of measurement data generates a high load in the system. There is also a danger that important error messages will be overlooked in the surge of measurement data.

As a result, the output of measurement data may only be selectively used for a limited number of access points simultaneously. The output release should only be used for a manageable period of time.

Generation



Configuration Management --> System Data --> IPDA --> Access point
Click **Search** and enable or disable the output of quality statistics on the **Quality of Service** tab in the **Signaling Quality of Service** section, then **Save**.



CHA-STMIB:MTYPE=NCUI2,TYPE=SIGQOS,LTU=99,QOSSTAT=NO;

The setting becomes effective immediately.

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

4.6.6 Error Messages from Quality Monitoring for the Signaling Connection over IP

4.6.6.1 F8289 - Output of Statistics Data

F8289 M4 N0367 NO ACT BPA TRANSSYS NET STATISTICS DATA 04-06-07 12:52:09
ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99 - ROUND TRIP DELAY VALUES
CONFIGURED : SHORT = 0800 LONG = 0400
AVERAGE : SHORT = 0520 LONG = 0000
HISTORY:
0500 0500 0500 0500 0610 0350 0350 0350 0350 0490
0160 0160 0160 0160 0130 0200 0200 0200 0200 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

Message contains statistical data concerning the message runtime (Round Trip Delay)

Measured values in the last 30 three-second intervals. Expressed in milliseconds, latest value first

Average values measures for the 15-second (SHORT) or the 60-second (LONG) interval. Specified in milliseconds.

Configured limits for the 15-second (SHORT) or the 60-second (LONG) interval. LONG in this case is the value set with the parameter MAXRTD and SHORT is 1.5x LONG. Expressed in milliseconds.

Time assignment of history data.
Zero values indicate intervals in which there were no packets to be sent

| 3 s | 6 s | 9 s | 12 s | 15 s | 18 s | 21 s | 24 s | 27 s | 30 s |
|------|------|------|------|------|------|------|------|------|------|
| 33 s | 36 s | 39 s | 42 s | 45 s | 48 s | 51 s | 54 s | 57 s | 60 s |
| 63 s | 66 s | 69 s | 72 s | 75 s | 78 s | 81 s | 84 s | 87 s | 90 s |

F8289 M4 N0368 NO ACT BPA TRANSSYS NET STATISTICS DATA 04-06-07 12:52:09

ALARM CLASS:CENTRAL:005

FORMAT:49

AP NUMBER: 99 - THROUGHPUT VALUES

CONFIGURED : SHORT = 0010 LONG = 0015

AVERAGE : SHORT = 0013 LONG = 0017

HISTORY:

| | | | | | | | | | |
|------|------|------|------|------|------|------|------|------|------|
| 0014 | 0014 | 0011 | 0013 | 0015 | 0016 | 0014 | 0015 | 0014 | 0017 |
| 0011 | 0014 | 0022 | 0023 | 0019 | 0018 | 0016 | 0025 | 0020 | 0030 |
| 0021 | 0041 | 0024 | 0035 | 0036 | 0025 | 0031 | 0034 | 0024 | 0018 |

Message contains statistical data concerning message throughput.

Average values measures for the 15-second (SHORT) or the 60-second (LONG) interval. Expressed in milliseconds.

Configured limits for the 15-second (SHORT) or the 60-second (LONG) interval. LONG in this case is the value set with the parameter MINTHRPT and SHORT is 2/3 of LONG. Expressed in milliseconds.

Measured values in the last 30 three-second intervals. Expressed in Kbps, latest value first

Time assignment of history data.
Zero values indicate intervals in which there were no packets to be sent

| 3 s | 6 s | 9 s | 12 s | 15 s | 18 s | 21 s | 24 s | 27 s | 30 s |
|------|------|------|------|------|------|------|------|------|------|
| 33 s | 36 s | 39 s | 42 s | 45 s | 48 s | 51 s | 54 s | 57 s | 60 s |
| 63 s | 66 s | 69 s | 72 s | 75 s | 78 s | 81 s | 84 s | 87 s | 90 s |

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

4.6.6.2 F8290 - Net Weakness Start Message Runtime Exceeded

F8290 M4 N0372 NO ACT BPA TRANSSYS NET WEAKNESS BEGIN 04-06-07 12:52:23
ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99 - ROUND TRIP DELAY VALUES
CONFIGURED : SHORT = 0800 LONG = 0400
AVERAGE : SHORT = 0590 LONG = 0410
HISTORY:
0580 0580 0580 0580 0640 0500 0500 0500 0500 0610
0350 0350 0350 0350 0490 0160 0160 0160 0160 0130
0200 0200 0200 0200 0000 0000 0000 0000 0000 0000
LONG INTERVAL VIOLATION

Start of net weakness
Message contains statistical data concerning the message runtime (Round Trip Delay)

Measured values in the last 30 three-second intervals. Expressed in milliseconds, latest value first

Reason for message - here: the limit for the 60-second (LONG) interval was exceeded

Average values measures for the 15-second (SHORT) or the 60-second (LONG) interval. Expressed in milliseconds.

Configured limits for the 15-second (SHORT) or the 60-second (LONG) interval. LONG in this case is the value set with the parameter MAXRTD and SHORT is 1.5x LONG. Expressed in milliseconds.

Time assignment of history data.
Zero values indicate intervals in which there were no packets to be sent

| 3 s | 6 s | 9 s | 12 s | 15 s | 18 s | 21 s | 24 s | 27 s | 30 s |
|------|------|------|------|------|------|------|------|------|------|
| 33 s | 36 s | 39 s | 42 s | 45 s | 48 s | 51 s | 54 s | 57 s | 60 s |
| 63 s | 66 s | 69 s | 72 s | 75 s | 78 s | 81 s | 84 s | 87 s | 90 s |

4.6.6.3 F8290 - Net Weakness Start Message Throughput Undershoot

F8290 M4 N0448 NO ACT BPA TRANSSYS NET WEAKNESS BEGIN 04-06-07 13:10:13

ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99 - THROUGHPUT VALUES
CONFIGURED : SHORT = 0010 LONG = 0015
AVERAGE : SHORT = 0013 LONG = 0014

HISTORY:
0014 0014 0011 0013 0015 0010 0014 0014 0014 0014
0011 0014 0012 0013 0014 0014 0009 0015 0013 0030
0021 0041 0024 0035 0036 0025 0031 0034 0024 0018

LONG INTERVAL VIOLATION

Start of net weakness
Message contains statistical data concerning message throughput.

Measured values in the last 30 three-second intervals. Expressed in Kbps, latest value first

Average values measures for the 15-second (SHORT) or the 60-second (LONG) interval.
Expressed in Kbps

Configured limits for the 15-second (SHORT) or the 60-second (LONG) interval. LONG in this case is the value set with the parameter MINTHRPT and SHORT is 2/3 of LONG. Expressed in Kbps.

Reason for message - here: the limit for the 60-second (LONG) interval was undershot

| 3 s | 6 s | 9 s | 12 s | 15 s | 18 s | 21 s | 24 s | 27 s | 30 s |
|------|------|------|------|------|------|------|------|------|------|
| 33 s | 36 s | 39 s | 42 s | 45 s | 48 s | 51 s | 54 s | 57 s | 60 s |
| 63 s | 66 s | 69 s | 72 s | 75 s | 78 s | 81 s | 84 s | 87 s | 90 s |

4.6.6.4 F8291 - Net Weakness End

F8291 M4 N0380 NO ACT BPA TRANSSYS NET WEAKNESS END 04-06-07
13:04:05
ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99

Configuring the IPDA Feature

Configuring Quality Monitoring for the Signaling Connection over IP

4.6.6.5 F8292 - Bandwidth Requirement Exceeds Limit

```
F8292 M4 N0284 NO ACT     BPA      TRANSSYS NET BW EXC BEGIN      04-06-07
12:41:13
ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99
LIMIT = 0040 KBIT/S
SHAPING TIME = 0011
```

Configured bandwidth to be set as limit
Expressed in Kbps

Time (in seconds) during which the number of messages to be sent exceeded the number permitted by the limited bandwidth

4.6.6.6 F8293 - Bandwidth Required Back Below Limit

```
F8293 M4 N0366 NO ACT     BPA      TRANSSYS NET BW EXC END      04-06-07
12:49:45
ALARM CLASS:CENTRAL:005
FORMAT:49
AP NUMBER: 99
```

4.7 Configuring Source Dependent Routing

With HiPath IP distributed architecture, it is possible to position parts of a HiPath 4000 system in different local networks. In this way, the HiPath 4000 CC could be located in Munich, with linked access points in Berlin and Frankfurt.

Now, if all calls were to be subject to uniform routing, this would result in a call from the Frankfurt access point being routed into the Frankfurt local network - with LCR from the point of view of the CC in Munich - via IP to Munich and from there back to Frankfurt as a long-distance call. This would not be particularly cost-effective.

If a subscriber at the access point in Berlin were to call the fire service, the call would arrive at the fire service in Munich, which would not only be prohibited, but also dangerous.

The solution to this problem is to assign the access points in Berlin and Frankfurt a connection to the respective local network and to route them on a subscriber-dependent basis.

This “source dependency“ always applies to multiple subscriber lines, CO circuits or tie trunk circuits. In order to identify a group requiring the same routing behavior, the source group ID is introduced. Every access point must be assigned to a source group. If the subscriber line, CO or tie trunk circuits are configured with source group ID “0“ (default value), they adopt the settings of the access point. If necessary, a source group ID which deviates from the access point can be assigned to individual subscriber lines, CO circuits or tie trunk circuits.

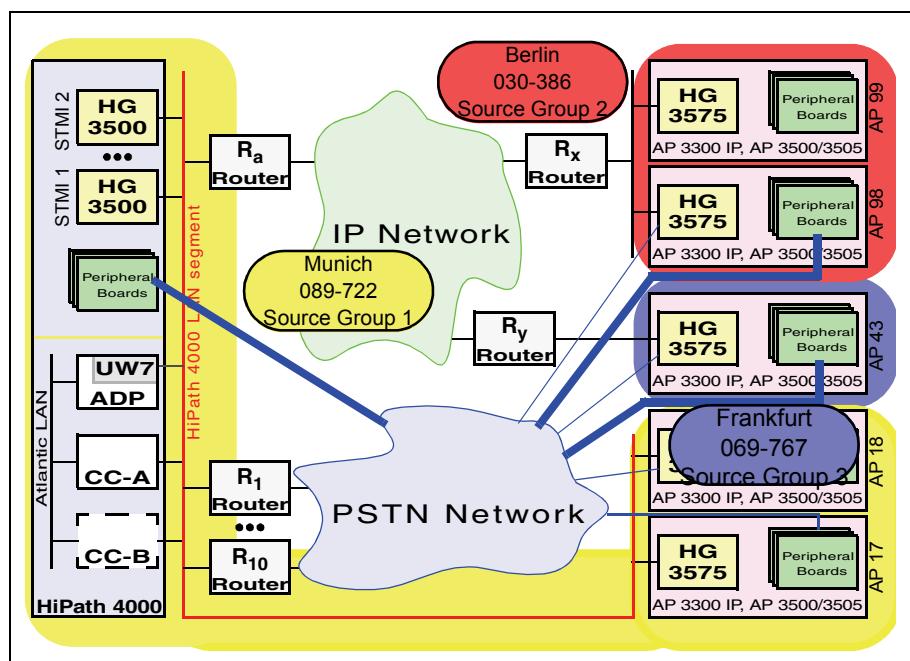


Figure 39

Source-dependent routing

Configuring the IPDA Feature

Configuring Source Dependent Routing

In the example, access points AP 17 and AP 18 in Munich have been assigned to Source Group 1, which is also always the default setting for all LTUs (1..15) of the central HiPath 4000 system. The two access points in Berlin (AP 98 and AP 99) have been assigned to Source Group 2. The Frankfurt access point AP 43 has Source Group 3.

The number of the source group is specified as the source group index with ADD-UCSU (see [Table 5 “SRCGRP” on page 4-60](#)).

In order to realize source dependent routing, LCR had to be extended.

While routing numbers (LROUTE) have previously been assigned in the digit pattern plan with the AMO LDPLN for one digit pattern, taking into account DPLN groups, class of service etc., source dependent routing requires that the index of an LCR profile (PROFIDX) be specified instead of the LROUTE. In the LCR profile, an LROUTE can be branched to as a function of the source group index. LCR profiles are configured with the AMO LPROF.

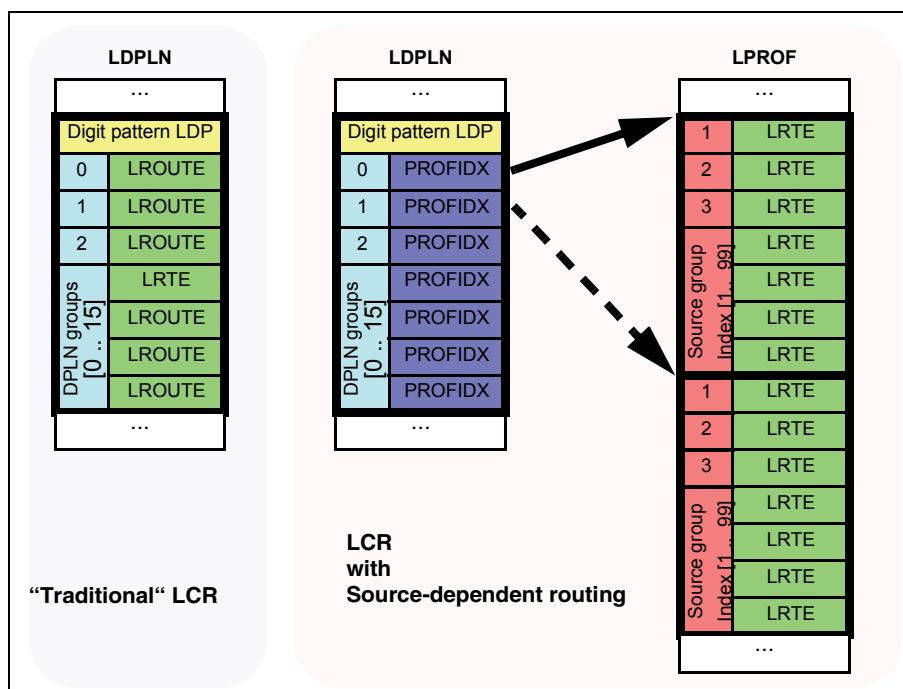


Figure 40 Interaction between LDPLN and LPROF

As PROFIDX indicates an LCR profile in the digit pattern plan, this must be configured first.

An LCR profile for emergency calls to the fire service is to be generated. In Munich, LRTE 722 leads to the CO; in Berlin, LRTE 386 and in Frankfurt, LRTE 767.



Configuration Management --> Least Cost Routing --> LCR Profiles
Click **New**, enter the **Profile Name**, **Source Group**, and **LCR Route** and **Save**.

The profile index is calculated and returned.



ADD-LPROF : PROFNAME=FEUERWEHR , SRCGRP=1 , LRTE=722 ;

The AMO returns the profile index, provided it is 12.
Additional source groups can be supplemented with:

CHANGE-LPROF : PROFIDX=12 , SRCGRP=2 , LRTE=386 ;
CHANGE-LPROF : PROFIDX=12 , SRCGRP=3 , LRTE=767 ;

Next, an entry can be made in the digit pattern plan for emergency calls to the fire service, indicating the LCR profile number 12 just configured.



Configuration Management --> Least Cost Routing --> Digit Pattern
Click **New**, enter **112** for **Digit Pattern**. On the **Data** tab, enter the **LCR Profile Number** configured above under profile index and **SAVE**.

ADD-LDPLN:LDP=112 , PROFIDX=12 , . . . ;

Additional functions of the AMO LPROF:



DELETE-LPROF : PROFIDX=12 , SRCGRP=3 ;

Deletes the entry for a source group from the specified LCR profile. If no source group is specified, the entire profile is deleted.



DISPLAY-LPROF : PROFIDX=1&&33 , INFOPAT=FEUER , FORMAT=K ;

All parameters are optional. A specific index or range can be specified for PROFIDX. INFOPAT allows a search pattern to be specified. If the pattern is found in a profile name, the profile is output. FORMAT is used to choose between short or long output format.

Notes:

- Every subscriber line, CO circuit or tie trunk circuit is automatically assigned the source group index 0 upon configuration. This means that the LTU source group index is used. However, it can be changed individually. A maximum of 99 source groups are available.
- The source group index used for a subscriber is output when the AMO SDAT is called up.
The output **SRCGRP = (1)** means that the subscriber uses the LTU source group index. The subscriber is configured with **SRCGRP=0**.
If the subscriber moves in an LTU that is assigned to another source group, it is assigned this source group.

Configuring the IPDA Feature

Configuring Source Dependent Routing

- The output SRCGRP = 1 means that the subscriber uses the value 1 independent of the LTU source group index. The subscriber is configured with SRCGRP=1.

The user-specific source group that is set thus remains the same if the subscriber moves to another LTU. Check if this allocation is still useful.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| LPROF | FORMAT | d | Abhängig vom Parameter Format werden die Profile in einem gekürzten Format angezeigt (nur die Service Information) oder in einem langen Format (alle für LCR Profile relevanten Informationen) K Ausgabe LCR Profile, Service Information - Kurz L Ausgabe LCR Profile Einträge - Lang. |
| | FORMAT | e | According to the parameter format, the profiles are displayed in a short format (only the Service Information) or a long format (all LCR profile related info). S Display LCR Profile, Service information - Short L Display of LCR Profile related info - Long |
| | INFOMUS | d | Bestimmt das Muster nach dem das Profil angezeigt wird. Wenn das im Parameter INFOMUS angegebene Muster im Profil Namen gefunden wird, wird das folgende Profil angezeigt. |
| | INFOPAT | e | Specifies the pattern according to which profiles will be displayed. If the pattern given in the INFOPAT parameter is found in the profile name, the following profile is displayed. |
| | LRTG | d | LCR Richtung |
| | LRTE | e | LCR route |
| | PROFIDX | d | LCR Profil-Index |
| | PROFIDX | e | LCR profile index |
| | PROFNAM E | d | LCR Profilname |
| | PROFNAM E | e | LCR profile name |
| | SRCGRP | d | Source Group Index |
| | SRCGRP | e | Source Group Index |

Table 16

AMO LPROF parameters

4.8 Configuring Payload Survivability

In principle, the HiPath 4000 IP distributed architecture is dependent on the availability of the IP network. If the IP connection fails between two access points or between the central HiPath 4000 switch and an access point, no payload connections are possible via IP.

Also, separation of signalling and payload streams is required very often by customers in the following scenario:

- signalling from branch to HQ should go over the IP Customer Network (WAN)
- payload should go over the traditional PSTN network using ISDN flatrate

The aspect of signalling between the CO and the access point has already been covered in [Section 4.5, “Configuring Signaling Survivability”, on page 112](#).

If control of the access point is safeguarded through signaling survivability, calls can be made within the access point in all cases. External calls via trunks or tie trunks in other systems are possible if the corresponding connection modules are located in this access point.

Payload survivability uses existing trunks in order to establish payload connections with other access points or with the HiPath 4000 central system independently of the IP network. In this context, the system calls itself via the trunk.

The procedure followed for payload survivability between a local subscriber and a CO/tie trunk circuit is route-specific.

If the call comes in via the CO/tie trunk circuit, a trunk call is established between the source group into which the call comes and the source group to which the subscriber belongs.

If, on the other hand, the HiPath 4000 subscriber establishes the call, the call is routed out of the system via the CO using LCR. A CO/tie trunk from the central system cannot be used in this case.

Payload survivability is destination-oriented and is restricted to one HiPath 4000 system. If other systems are connected to the HiPath 4000, the networking LCR must be extended. Details can be found in [Section 4.8.4, “Payload Survivability in HiPath 4000 Networks”, on page 165](#).

4.8.1 When is Payload Survivability Used?

There are the following reasons to handle connections to access points via trunk traffic instead of via IP:

- a) If the quality of the existing connections in the IP network is bad
- b) The capacity of the IP link is exhausted
- c) If a subscriber specifies via access code that he does not wish to use IP
- d) All payload routes between the HiPath host system (all HiPath HG 3500 modules) and an access point are labeled as „Bad Quality“ as soon as signalling survivability is activated for the access point.

NOTE: In case of alternative routing (signaling survivability is active) the payload matrix between HHS and the corresponding AP will be blocked. All available routes from HHS to AP are marked as BAD IP.

- e) If in AMO UCSU parameter BCHLCNT is set to „0“.

If the quality of the existing connections in the IP network is bad

The quality of the active payload connections via the IP network is permanently monitored.

If the packet delay or the packet loss rate exceeds the predefined or upper limits, the connection is labeled as „Bad Quality“. If these variables drop below the likewise predefined lower limits, the connection is relabeled as „Good Quality“. The limit values are set in the **PLQUAL** branch in AMO SIPCO (see [Section 4.1, “Payload Quality \(PLQUAL\)”, on page 53](#)).

Figure 41 indicates the sequences:

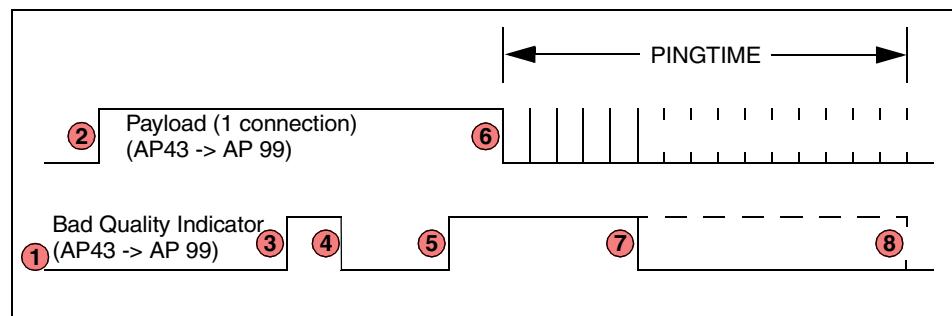


Figure 41 *Blocks the IP connection for payload due to „Bad Quality“*

- 1 At the start of appraisal, the IP connection quality of AP 43 to AP 99 is labeled as good.
- 2 A payload connection is established via IP.

3 The constant monitoring of the connection quality reports “Bad Quality”

From this time on, no further payload connections are established between AP 43 and AP 99 via IP. If available, an alternative route via payload survivability is used. Otherwise, the connection request is rejected.

The existing payload connection is not disconnected, despite “Bad Quality”.

4 The constant monitoring of the connection quality reports a return to “Good Quality”

The establishment of payload connections between AP 43 and AP 99 over IP resumes from this time on.

5 as per 3

6 The subscriber terminates the payload connection

At this time, the connection is labeled as “Bad Quality”.

As a result of the preceding payload connection, “UDP ping” messages are now transmitted every 5 seconds, in order to further monitor the behavior of the IP connection.

7 The test with “UDP ping” messages shows that the connection quality has been restored.

The “Bad Quality indicator” is reset.

From this time on, payload connections are again established between AP 43 and AP 99 via IP.

8 If the tests with “UDP ping” messages are unsuccessful, the “bad quality indicator” is reset after expiry of PINGTIME.

PINGTIME is configured in the TIMING branch of the AMO SIPCO. The value range is between 0 and 3600 seconds.

If several payload connections are running in parallel between 2 access points or between an access point and HG 3500, these may provide differing quality statements. In all events, the „Bad Quality“ status of a connection is always prioritized over any number of „Good Quality“ connections.

In other words, if 10 connections report „Good Quality“ and 1 reports „Bad Quality“, no further IP connections are established until the connection with the status of „Bad Quality“ has returned to a status of „Good Quality“. For information on possible sequences, see [Figure 41 “Blocks the IP connection for payload due to „Bad Quality“”](#).

All payload routes between the central system (all HiPath HG 3500 modules) and an access point are labeled „Bad Quality“ as soon as signaling survivability is activated for the access point. In this case it is assumed that a fault affecting the route between the central system and access point is having the same effect on the payload connections.

If the blocking of the availability of subscriber lines in an access point without payload survivability due to poor IP connections is to be prevented („Bad Quality“), payload quality handling can be deactivated for the access point in the AMO UCSU with the parameter **PLCHECK**. This means that every call is switched regardless of the quality of the IP connection. In the worst case scenario, this can result in the call being signaled, but the voice link remaining dead because no packets with payload are received.

The capacity of the IP link is exhausted

The transport capacity for payload connections between an access point and the IP network is limited by the maximum number of simultaneous connections possible (30/60/120 connections depending on the hardware) and the maximum bandwidth configured in the Resource Manager. If the full transport capacity is used, the payload survivability route is automatically used for further calls within the HiPath 4000 system. The path selection makes no distinction as to whether there is no path available because of a failure in the IP network or because all available routes from the access point are already occupied.

Because of the restrictions with regard to payload survivability, the system must be configured so that this spillover route is only used in cases of exceptional overload.

If a subscriber specifies via access code that he does not wish to use IP

In Hipath 4000 system, the WABE code **FRCALTRT** can be used to force the survivability route. The access code **FRCALTRT** can be used by anyone and is not subject to any class of service requirements. The same payload survivability restrictions apply for these calls.

4.8.2 Possible Features

Payload survivability is a backup service that operates in the event of faults in the IP network. The alternative route via the CO restricts the features available.

The following features are supported:

- Fax-Modem
- Hunt Group

Hunting group stations are reached over LAN if calling party and hunt group member are in the same shelf. In case that calling party and hunt group member are in a different shelf hunting group station is reached over Central Office.

- Call Forwarding

The user can forward calls to a party located on a different shelf.

- Call forwarding busy/no answer is possible in the same system. To stations located on a different shelf the call will be routed over CO.
- Call forwarding to Xpressions is possible independent of shelf location when a TIE trunk is configured.
- Call forwarding to a station configured on closed numbering will be possible independent of shelf location when a TIE trunk to the other system is configured.

- Transfer and Toggle

Transfer of incoming and outgoing external calls is possible to stations located on a different shelf. These calls are routed over CO.

- Keyset
- Call Waiting
- Call Pick Up

Depending on the called party a CO connection is used.

- For call scenarios where calling, called and picking party are on the same shelf no CO route is used.
- For call scenarios where calling party and called party and picking party are on another shelf CO route is used.
- For call scenarios where calling and called party are on the same shelf and picking party is located on a different shelf 2 CO routes are used.
- Call Log
- Call Back

A station user can set a call back request to a party located on a different shelf.

- Callback on busy is possible for calls between different shelves over CO.
- Callback on no answer is possible for calls between different shelves over CO.
- One Number Service (ONS)
- Conference
- Name Display
- Number Display
- Direct Station Selection (DSS)
- Camp on
- Busy override
- OpenScape Xpressions

The following Xpressions scenarios are possible independent of shelf location when a TIE trunk to Xpression is configured:

- Direct call to Xpression
- Call forward to Xpression
- Message waiting indication
- Transfer out from Xpression
- Listen to recorded voice mails using mailbox key

Restrictions:

- The new features are only supported with **ALR via multichannel trunk circuit under one call number**. ALR with single number and PUBDID are not supported.
- Pick up group configuration with distributed members is not recommendable due to CO resources usages.
- Different trunk groups must be configured for payload separation without intercept parameters.
- Route optimization is not possible.
- Direct tie trunk access if the trunk is located on different shelf is not possible.
- FWD for Hunt Group members is not supported.
- Announcement with hunting group call queue is not supported due to CO resource limitations.

- Group call is not supported due to resources allocation.
- Networkwide call pickup groups are not supported.
- The mailbox station number must be dialed after the call when it is forwarded to Xpression over CO.
- Keyset station cannot pickup a call from a secondary line.
- Calls to attendant are not possible.
- External applications using ACL (through CAP/CA4000) except ComAssistant will be restricted due to the different call ID for a call performed over payload survivability.
- VNR environment is not considered in Step 1 Release.
- DSS is not supported in Step 1 Release.
- Override/Intercept are not supported in Step 1 Release.
- Camp on is not supported in Step 1 Release.
- Analog trunk as TIE is not supported due to signaling delays.
- Synchronized announcement is not supported due to the CO resource usage.
- MLPP is not supported - MLPP calls over payload separation are not possible.
- Chese - Secretary and Executive located on different source groups - secretary receive busy tone. No notification for station B executive.
- Broadcast, Speaker Call - One-Way is not supported.
- ACD agent located in another source group cannot pickup the call.
- Park: Station from different source group can not connect to parked call. The user sees on the display that is connected to calling station but cannot hear anything. Calling station is on hold state

4.8.3 How is Payload Survivability Configured?

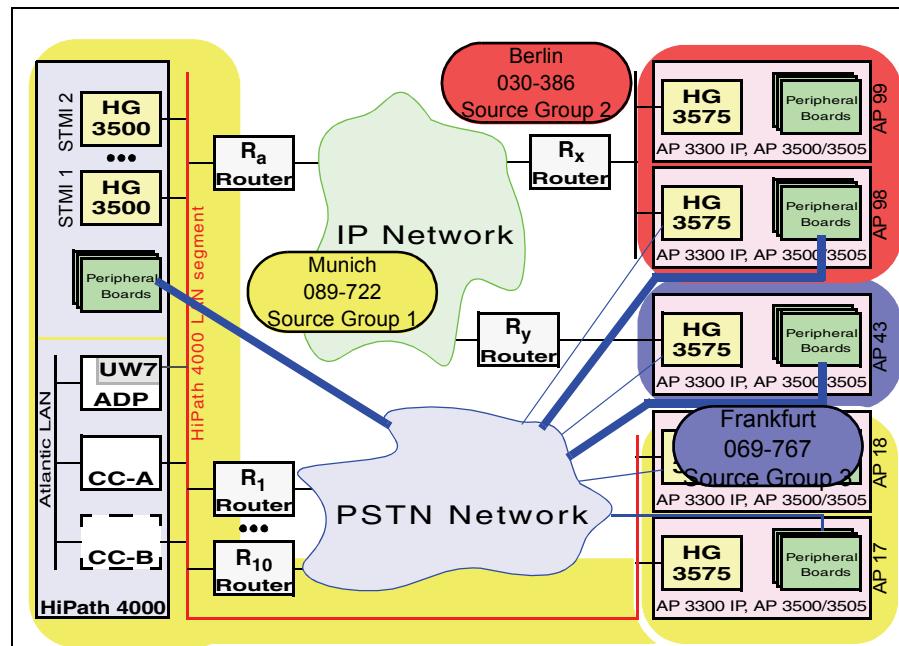


Figure 42 Payload survivability - source dependent routing configuration

Payload survivability requires CO lines at access points, in order to switch alternative routes. If, in example [Figure 42 “Payload survivability - source dependent routing configuration”](#), the IP connection between Berlin and Frankfurt fails, all existing calls will be interrupted. No new calls can be set up until “Good Quality” has been determined again.

As both an access point in Berlin and the access point in Frankfurt have a local CO line, calls between subscribers in Berlin and Frankfurt can alternatively be switched via the trunk. Of particular note here is that, in the case of HiPath IPDA, a HiPath 4000 system now calls itself via trunk, in order to connect its own subscribers.

The alternative routes are defined as a function of the source group. Thus, in the example, it is unnecessary for AP 99 to have its own trunk access. It can be reached via the trunk access of its source group in AP 98.

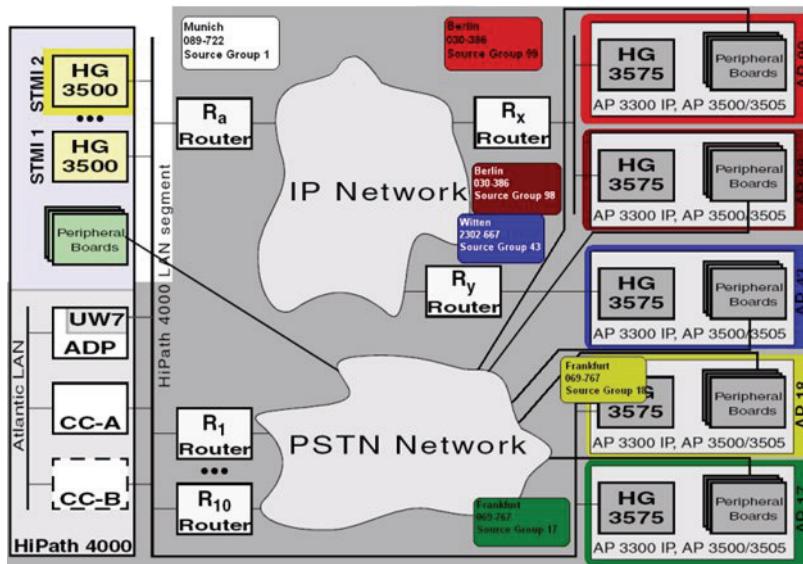


Figure 43

Payload survivability with all access points configured in different source group

In this situation (refer to [Figure 43 “Payload survivability with all access points configured in different source group”](#)) all access points have to be assigned in different source group and CO will be mandatory for all APs. All calls between access points will be made over ISDN lines.

New AMO parameters in AMO ZAND and ZANDE from HiPath 4000 V5 on

- Parameter **NPLSURV**: (default set to NO)

This parameter is irrelevant for HiPath 4000 SoftGates. It only affects traditional IPDA shelves.

When parameter **NPLSURV** is set to **NO** (default) then we have the traditional behavior that we had up to Hipath 4000 V4.

When parameter **NPLSURV** is set to **YES** then the traditional behavior will be enhanced according to parameter **PLMSGSRV**.

For detailed description of all possible combinations of parameters **NPLSURV** and **PLMSGSRV** see description of parameter **PLMSGSRV**.

- Parameter **PLMSGSRV**: (default set to YES)

This parameter's effect depends on the AP type; whether it is a HiPath 4000 SoftGate or a traditional IPDA shelf (e.g AP37009).

For a traditional IPDA shelf, parameter **NPLMSURV** will be checked. However for a HiPath 4000 SoftGate, parameter **NPLMSURV** is irrelevant and will not be checked.

- Traditional IPDA shelf:

If **NPLMSURV** is set to **NO** then parameter **PLMSGSRV** is irrelevant. That means that when the IPDA shelf is in signalling survivability then only the connection to HHS will be blocked in **PLMATRIX**. This is the traditional behavior that we had up to HiPath 4000 V4.

NPLMSURV is set to **YES**, **PLMSGSRV** is set to **YES** (default) and the IPDA shelf is in Signalling Survivability: **PLMATRIX** from this IPDA shelf to HHS and all other APs **except** those in the same source group will be blocked.

NPLMSURV is set to **YES**, **PLMSGSRV** is set to **NO**, and the IPDA shelf is in Signalling Survivability: **PLMATRIX** from this IPDA shelf to HHS and all other APs (regardless of the source group) will be blocked.

– HiPath 4000 SoftGate:

If the HiPath 4000 SoftGate is in Signalling Survivability and parameter **PLMSGSRV** is set to **YES** (default) then **PLMATRIX** from this HiPath 4000 SoftGate to HHS and all IPDA shelves which are not in the same source group will be blocked.

If the HiPath 4000 SoftGate is in Signalling survivability and parameter **PLMSGSRV** is set to **NO** then **PLMATRIX** from this HiPath 4000 SoftGate to HHS and all IPDA shelves (regardless of the source group) will be blocked.

There are 3 variants of payload survivability, which depend on the type of trunk switching and have different advantages and disadvantages. ALR should be used as standard.

ALR with single number Functions with any kind of trunk switching, even analog.

- A separate phone number must be assigned to each channel of the trunk switching
 - Therefore requires many individual phone numbers and many entries in the ALTROUT table
 - Call charges for using the payload survivability route cannot be uniquely assigned to the calling party
 - When the payload survivability route is used, party A sees the “Alternate Routing Number” used for the call in addition to the dialed internal number
 - When the payload survivability route is used, party B hears the “external call ring” despite the fact that it is an internal call, but sees the internal phone number of party A.
-

| | |
|---|--|
| ALR via multichannel trunk circuit under one call number | <p>Only functions with multichannel ISDN CO lines.</p> <ul style="list-style-type: none"> Only one phone number for all of the channels of a circuit Only one entry per circuit in the ALTROUT table Use of the “Artificial Calling Number” requires agreement with the PSTN network carrier that the transmitted calling party number will not be checked, as it does not correspond to the actual phone number for the circuit (USER PROVIDED SCREENED). The same must be agreed for all source groups. The source group for which ALR is configured with ARTCNR must be available in this way from all other source groups. The entire carrier network must guarantee transmission of the Artificial Calling Number from all source groups without corruption. (No modification of the phone number) Call charges for using the payload survivability route cannot be uniquely assigned to the calling party When the payload survivability route is used, party A sees the “Alternate Routing Number” used for the call in addition to the dialed internal number When the payload survivability route is used, party B hears the “external call ring” despite the fact that it is an internal call, but sees the internal phone number of party A. |
| PUBDID | <p>If PUBDID numbers are already configured for subscribers of an access point, these can also be used for payload survivability.</p> <ul style="list-style-type: none"> Relatively high level of administration effort involved, as the PUBDID number has to be configured individually for each subscriber. 1 entry in the ALTROUT table for the entire source group The PUBDID number is retained in the event of a relocation In the case of payload survivability, the PUBDID number is displayed for the other party Call charges for using the payload survivability route can be uniquely assigned to the calling party |

ALR with single number

At the CO line which is (also) to be used for the payload survivability of a source group, certain call numbers are configured for payload survivability.

Configuring the IPDA Feature

Configuring Payload Survivability

Let us assume that the numbers 069-767-97, 069-767-98 and 069-767-99 have been reserved in Frankfurt for payload survivability. Up to 3 calls can then reach source group 3 simultaneously via alternative routes.

The INCALTRT digit analysis result must be configured in WABE for every access code.

This is configured through



Configuration Management --> System Data --> IPDA --> IPDA Payload Survivability

Click **New**, enter **Index**, **Routing Position**, **Phone Number** and **Access Code** on the **Basic Data** tab and **Save**.

Configuration Management --> Tables --> Dial Plan --> Dial Codes

Click **New**, select **Delete Mask** on the **Edit** pull-down menu.
Enter the **Dial Code** and **Code Type** and **Save**.



ADD-APRT : TYPE=ALTROUT , SRCGRP=3 , POS=1 , ALRTYPE=ALR ,
ALTRTNR=006976797 , ACCODE=97 ;
ADD-WABE : CD=97 , DAR=INCALTRT ;

ADD-APRT : TYPE=ALTROUT , SRCGRP=3 , POS=2 , ALRTYPE=ALR ,
ALTRTNR=006976798 , ACCODE=98 ;
ADD-WABE : CD=98 , DAR=INCALTRT ;

ADD-APRT : TYPE=ALTROUT , SRCGRP=3 , POS=3 , ALRTYPE=ALR ,
ALTRTNR=006976799 , ACCODE=99 ;
ADD-WABE : CD=99 , DAR=INCALTRT ;

This insertion sequence means that ACCODE 97 is at the top of the list and is occupied first.

Note regarding ALTRTNR

Specific rules must be observed for the Alternate Routing Number ALTRTNR:

- ALTRTNR must contain the access code for CO breakout.
- If the source groups are distributed across different local networks, the local network access codes must also be specified (see example).
- The access code setting for CO breakout must be identical in all source groups. The destination number must be accessible in the same way from all other source groups.
- ALTRTNR cannot be modified throughout the entire network with LCR (no REROUTE-INTERN).
- ALTRTNR must be routed in each source group on a “source-dependent” basis.

Note regarding AMO parameter POS (AMO APRT:ALTROUT)

The AMO parameter POS is optional. If this parameter is not specified, the entry is inserted at the end. The table is always kept compact starting at POS=1. If a specific POS value is specified, the table entry is only entered at this position if

this position is already occupied or if it is the first free position. If this position is not free, the entries following POS are shifted back. If this position is not free, the entries following POS are shifted back.

If an entry is deleted, all subsequent entries are shifted forward by one position. POS is important when multiple entries are made for a source group. Assignment of the specified alternative routes is in ascending order according to the POS value.

ALR via multichannel trunk circuit under one call number

At the CO line, 30 channels are available, for example, to a source group for payload survivability, all of which can be reached via the same call number. In Munich, for example, this could be the number 089-722-9000.

The INCALTRT digit analysis result must be configured in WABE for the access code 9000.

Furthermore, up to 30 calls, for example, can reach source group 1 simultaneously via alternative routes. However, as all calls are routed to the same call number (ACCODE, AMO APRT:ALTROUT), the call processing is faced with the problem of correctly assigning the alternative route calls. To this end, an identification number has to be transmitted with each call. This is realized by replacing the Calling Party Number. Precisely which numbers will be available to this end is configured via the parameters ARTCNR (Artificial Calling Number) and ARTCNRG (Artificial Calling Number Range).

The Artificial Calling Number is configured on a target-dependent basis with the information on a specific source group. However, this number is used at the source, i.e. at the trunk access which leads into the alternative route. The value is ultimately used as the Calling Party Number. As carriers do not allow freely selectable Calling Party Numbers, an agreement must be made with the carrier concerning the use of the Artificial Calling Numbers). The carrier must deactivate checking of the Calling Party Number (CLIPNOSCREEN).

Configuration example:



Configuration Management --> System Data --> IPDA --> IPDA Payload Survivability

Click **New**, fill in all fields for alternative routing on the **Basic Data** tab and **Save**.

Configuration Management --> Tables --> Dial Plan --> Dial Codes

Click **New**, select **Delete Mask** on the **Edit** pull-down menu. Enter the **Dial Code** and **Code Type** and **Save**.



**ADD-APRT:TYPE=ALTROUT , SRCGRP=1 , ALRTYPE=ALR ,
ALTRTNR=00897229000 , ACCODE=9000 , ARTCNR=1000 ,
ARTCNRG=30 ;**

ADD-WABE:CD=9000 , DAR=INCALTRT ;

Note regarding ARTCNR

Specific rules must be observed for the Artificial Calling Number ARTCNR:

Configuring the IPDA Feature

Configuring Payload Survivability

- The ARTCNR ranges for different circuits and source groups must not overlap.
- The ranges must be big enough to allow the desired maximum number of calls via the payload survivability route on a circuit.
- This ARTCNR range must **NOT** be reserved in WABE.
- The entire carrier network must guarantee transmission of the ARTCNR range from all source groups without corruption. (No modification of the phone number)

PUBDID

Subscribers of a source group have a Public DID number in the local CO. In other words, Berlin-based subscribers can be reached directly both via the central HiPath 4000 switch's Munich dial-in and via their Berlin dial-in number. For example: a subscriber could be reached not only via 089-722-**12345**, but also via 030-386-**789** (different extension numbers/branch concept).

Setting the PUBDID number: *[TON: Type Of Number - NPI: Numbering Plan Identifier]*



Configuration Management --> Station --> Station
Click **Search** and go to subscriber. Enter the **Station No., Numbering Plan Identifier** and **Type of Number (TON)** on the **Basic 3** tab under **Primary Rate Interface** and **Save**.



CHANGE-SDAT:STNO=12345,TYPE=DATA1,PUBNUM=30386789,
TON=NATIONAL,NPI=ISDN;

Other settings made using the AMOs DNIT and DIDCR are required.

If this mechanism for payload survivability is to be used, it is activated as follows:



Configuration Management --> System Data --> IPDA --> IPDA Payload Survivability
Click **New**, enter the **Position** and **Type Of Routing** on the **Basic Data** tab and **Save**.



ADD-APRT:TYPE=ALTROUT,SRCGRP=2,POS=1,ALRTYPE=PUBDID;

However, it is also possible to configure one of the ALR procedures for payload survivability for source groups.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|------|-----------|----------------------|---|
| APRT | SRCGRP | d | Source Group Index Zuordnung des Access Points in eine Source Group. Die Access Points einer Source Group sind für Payload Survivability über einen bestimmten Amtsanschluss erreichbar. |
| | SRCGRP | e | Source Group Index Assignment of the Access Point to a Source Group. The Access Points of one Source Group are reachable via a distinct CO trunk for Payload Survivability. |
| | POS | d | Position Index des Eintrags in der Alternate Routing Tabelle. [1 .. 500] Siehe auch: Section 4.8.3, “Note regarding AMO parameter POS (AMO APRT:ALTROUT)”, on page 160 |
| | POS | e | Position Index of the entry in the Alternate Routing Table. [1 .. 500] See also: Section 4.8.3, “Note regarding AMO parameter POS (AMO APRT:ALTROUT)”, on page 160 |
| | ALRTYP | d | Alternate Routing Typ des Eintrags. 3 Typen sind möglich: ALR: Alternate Routing über eine DID, DIT oder PRI Nummer. NOALR: Kein Alternate Routing Pfad PUBDID: Alternate Routing über Public DID Nummer, d.h. Teilnehmer haben eine zweite Nummer, unter der sie über den Amtsanschluss für die angegebene Source Group aus dem öffentlichen Netz erreichbar sind. |
| | ALRTYPE | e | Alternate Routing Type of the Entry 3 types are possible: ALR: Alternate Routing via a DID, DIT or PRI number. NOALR: No Alternate Routing PUBDID: Alternate Routing using a public DID number. Subscribers are reachable by a second number via the CO access for the specified Source Group. |
| | ALTRTNR | d | Rufnummer für Alternate Routing Vollständige Rufnummer des Alternate Routing Anschlusses Siehe auch: Section 4.8.3, “Note regarding ALTRTNR”, on page 160 |

Table 17

AMO APRT parameters in ADD branch under TYPE=ALTROUT

Configuring the IPDA Feature
Configuring Payload Survivability

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | ALTRTNR | e | Alternate Routing Number. Complete number of the Alternate Routing access See also: Section 4.8.3, “Note regarding ALTRTNR”, on page 160 |
| | ACCODE | d | Access Code Nebenstellennummer des Alternate Routing Anschlusses, d.h. ALTRTNR ohne Vorwahl und Amtsnummer. Maximal 6-stellig. |
| | ACCODE | e | Access Code Extension Number of the ALternate Routing Access. ALTRTNR without Area and Office Code. Maximum 6 digits. |
| | ARTCNR | d | Artificial Calling Number Maximal 6-stellige Nummer, welche zur Identifikation des Rufes als “Nummer des Rufenden” übertragen wird. Diese Nummer ist die erste eines Bereichs (siehe ARTCNRNG), der für diese Zwecke genutzt wird. Siehe auch: Section 4.8.3, “Note regarding ARTCNR”, on page 161 |
| | ARTCNR | e | Artificial Calling Number. A number with a maximum of 6 digits. Is given als “Calling Party Number” to identify the call. This number is the first of a range (see ARTCNRNG) used for that purpose. See also: Section 4.8.3, “Note regarding ARTCNR”, on page 161 |
| | ARTCNRNG | d | Artificial Calling Number Bereich Gibt an, wieviele Artificial Calling Numbers einschließlich ARTCNR zur Verfügung stehen [1 .. 99999]. |
| | ARTCNRNG | e | Artificial Calling Number Range Specifies, how many Artificial Calling Numbers including ARTCNR are available [1 .. 99999]. |

Table 17 AMO APRT parameters in ADD branch under TYPE=ALTROUT

4.8.4 Payload Survability in HiPath 4000 Networks

Payload survivability is destination-oriented and is restricted to **one** HiPath 4000 system. If other systems are connected to the HiPath 4000 via ECMAV2 trunks (closed numbering), the networking LCR (NWLCR) must be extended. Otherwise, AP subscribers cannot access the relevant network subscribers when payload survivability is active.

The procedure followed for payload survivability between a local subscriber and a CO/tie trunk circuit is route-specific.

If the call comes in via the CO/tie trunk circuit, a trunk call is established between the source group into which the call comes and the source group to which the subscriber belongs.

If, on the other hand, the HiPath 4000 subscriber establishes the call, the call is routed out of the system via the CO using LCR. A tie trunk from the central system cannot be used in this case.

[Figure 44 “Payload survivability and networking - normal route A calls B or B calls A”](#), [Figure 45 “Payload survivability and networking - survivability route A calls B”](#) and [Figure 46 “Payload survivability and networking - survivability route B calls A”](#) show the different routes.

To handle call A -> B with payload survivability ([Figure 45 “Payload survivability and networking - survivability route A calls B”](#)), an extension must be added to the NWLCR of system 1 for the route to DESTNO 2. This extension contains an overflow entry to the local CO of AP 17 (trunk group 17), which ensures that routing to destination system 2 takes place via CO in the case of payload survivability.

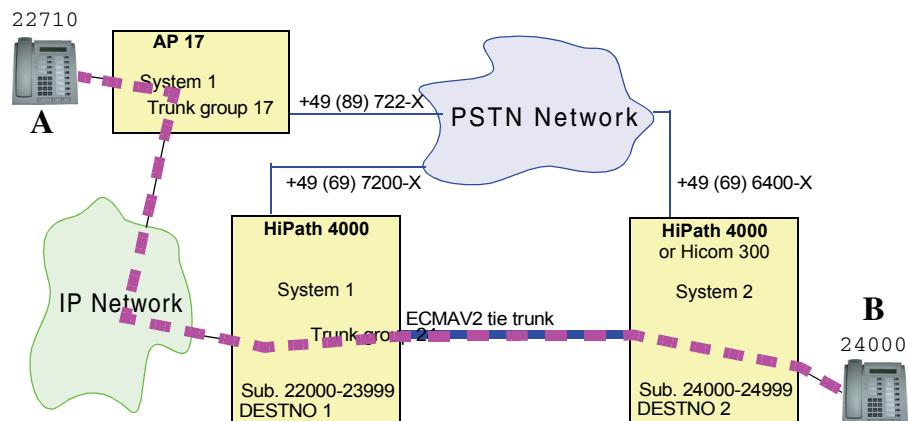


Figure 44

Payload survivability and networking - normal route A calls B or B calls A

Configuring the IPDA Feature

Configuring Payload Survivability

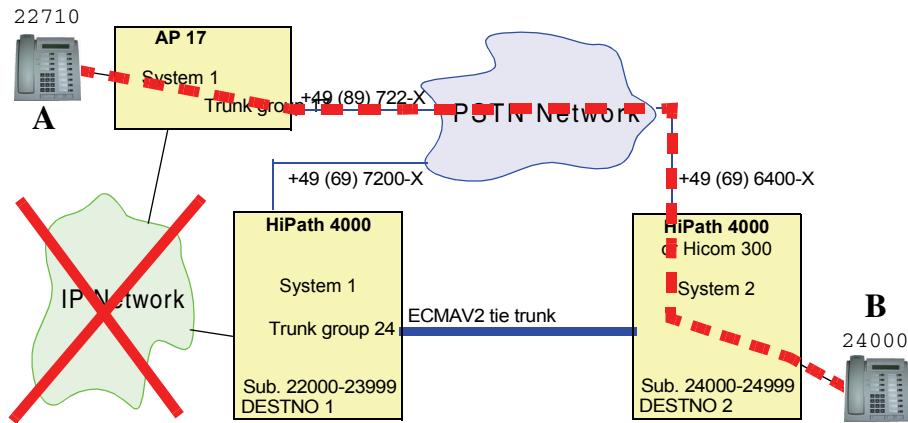


Figure 45 Payload survivability and networking - survivability route A calls B

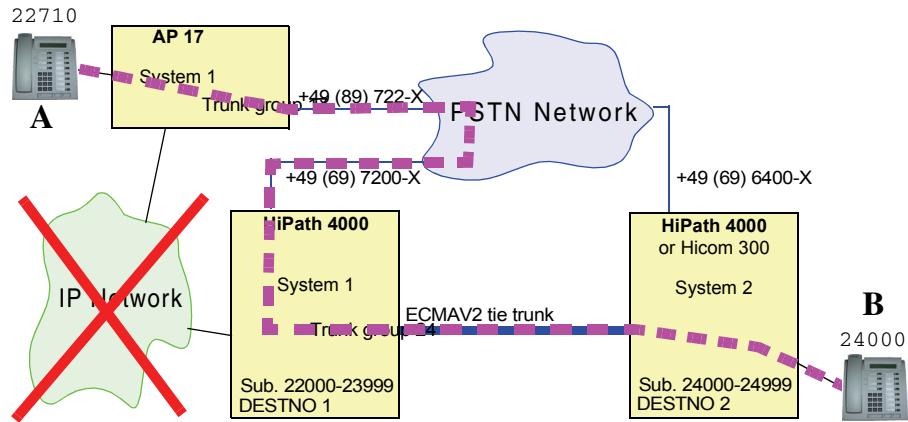


Figure 46 Payload survivability and networking - survivability route B calls A

NWLCR extension for AP 17 to system 2 with payload survivability (Figure 45 "Payload survivability and networking - survivability route A calls B")

```
+-----+
| LRTE = 124          NAME = SYSTEM 2          SERVICE = ALL |
| TYPE = NWLCR        |                         DIDNO-ROUTE = 1 -2 -400 |
| SERVICE INFO =      |                         |
+-----+-----+-----+-----+-----+-----+-----+-----+
|     |     |     |     |     | SCHEDULE | CARRIER   |     |     |
| LRTGEL | LVAL | TRUNO | LWR | LBER | ABCDEFGH | ZONE    | LATTR | LDSRT |
+-----+-----+-----+-----+-----+-----+-----+-----+
|     1 |     1| 24 | 1 | 1 | *****   | 1 | EMPTY | NONE |     |
|     2 |     1| 17 | 17| 17 | *****   | 1 | EMPTY | NONE |     |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| LWR      LWRELPOS LWREL      PARAMETER |
+-----+
| 1       | 1       ECHO     1           |
|       | 2       END      |
+-----+
```

Configuring the IPDA Feature

Configuring Payload Survivability

```
+-----+-----+
| INFO:STANDARD NWLCR FOR SYSTEM 2 |
+-----+
+-----+
| LWR      LWRELPOS  LWREL      PARAMETER   |
+-----+
| 17       1        OUTPULSE   696400    |
| 2         |        ECHO      1          |
|           |        3        NPI       ISDN      |
|           |        4        TON       NATIONAL  |
|           |        5        END      |
+-----+
| INFO:OVERFLOW CO FOR SYSTEM 2 (SURVIVABILITY) |
+-----+
```

Configuring the IPDA Feature

Configuring Subscriber, CO/Tie Trunk Circuits in Access Points

4.9 Configuring Subscriber, CO/Tie Trunk Circuits in Access Points

In an IP distributed access point, all subscriber line and CO/tie trunk modules can be used, with a few exceptions which are described in the HiPath 4000 Technical Upgrade Plan

When using analog access modules which also require a ring generator, the following must be taken into consideration:

In the 19" access point HiPath AP 3500 IP and the AP 3505 IP expansion box, only RGM type ring generator modules (S30807-Q6141-X or S30122-K5929-X) can be used, not RG modules. The HiPath AP 3505 IP expansion box requires its own RGM independently of the AP 3500 IP basic box, if analog access modules are to be operated in it.

NOTE: Trunk connections between access points in the same system or between a central system and its access points are not permitted.

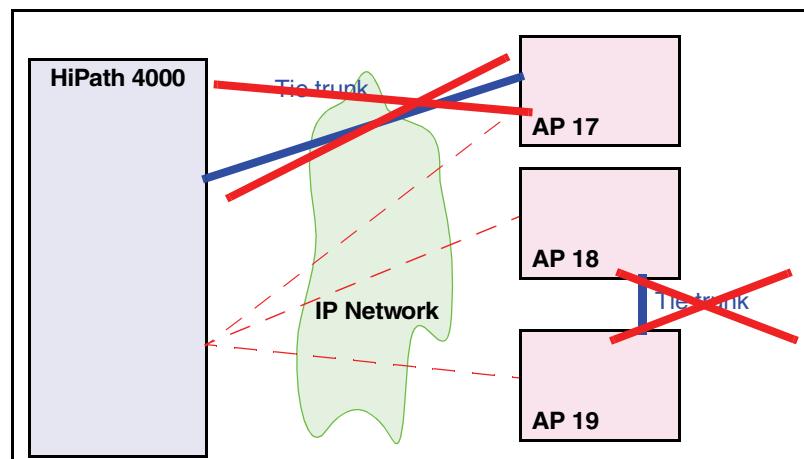


Figure 47 Tie connections are not permitted within a system

With the configuration in an IP distributed access point, all circuits are given additional parameters to govern their handling of Voice over IP. These IPDA classmarks are:

| Classmark | Sprache/ Language | Beschreibung/ Description |
|-----------|----------------------|---------------------------|
| EC | d | Echo Cancellation |
| EC | e | Echo Cancellation |
| G711 | d | Codec Typ G.711 |
| G711 | e | Codec Type G.711 |
| G729 | d | Codec Typ G.729A |

Table 18

HiPath 4000 IPDA classmarks

| Classmark | Sprache/ Language | Beschreibung/ Description |
|-----------|----------------------|--|
| G729 | e | Codec Type G.729A |
| G729OPT | d | Codec Typ G.729A - optional |
| G729OPT | e | Codec Type G.729A - optional |
| INIT | d | stellt Default-Einstellung wieder her |
| INIT | e | restores default setting |
| KEINE | d | schaltet alle Classmarks aus |
| NONE | e | turns all Classmarks off |
| ML | d | Multiple Listener - Ansage wird auf einer Verbindung übertragen und im Access Point an mehrere Sätze geschaltet. *) nur für Ansagegeräte/MOH |
| ML | e | Multiple Listener - Announcement is transmitted on a single connection and switched to multiple ports in the Access Point. *) only for Announcement Devices/MOH |
| VAD | d | Voice Activity Detection |
| VAD | e | Voice Activity Detection |
| VIAHHS | d | Payload über Zentralsystem *) nur für Ansagegeräte/MOH |
| VIAHHS | e | Payload via central system *) only for Announcement Devices/MOH |

Table 18 HiPath 4000 IPDA classmarks

Details of the procedures that are switched with classmarks can be found in:

- [Voice Compression](#) - [Section 5.3 on page 5-52](#) in the document “HiPath Gateways HG 3500 and HG 3575”
- [Voice Activity Detection \(VAD\)](#) - [Section 5.4 on page 5-53](#) in the document “HiPath Gateways HG 3500 and HG 3575”
- [Echo Cancellation](#) - [Section 5.6 on page 5-54](#) in the document “HiPath Gateways HG 3500 and HG 3575”
- [Codec Standards](#) - [Section 2.3 on page 2-12](#) in the document “HiPath Gateways HG 3500 and HG 3575”

Handling the classmarks for a call

If a call is to be established between Subscriber A and Subscriber B, the classmarks of both subscribers, or of the subscriber and the CO/tie trunk circuit via which the subscriber is reached, are assessed.

Echo cancellation or voice activity detection is only activated if both circuits have set the corresponding classmark.

Configuring the IPDA Feature

Configuring Subscriber, CO/Tie Trunk Circuits in Access Points

Connections with announcement devices configured with the AMOs SSC, RCSU or TSCSU are an exception to this rule. Here, the announcement device setting is always adopted.

| EC or VAD | | Circuit B | | AnnouncementDevice (RCSU) | |
|-----------|-----|-----------|-----|---------------------------|-----|
| | | NO | YES | | |
| Circuit A | NO | NO | NO | NO | YES |
| | YES | NO | YES | | |

Table 19 Classmark handling for EC or VAD

In the case of codec types, only one type which supports both is selected.

In contrast to version 1, compression is now available for announcement devices and conferences. As far as codec classmarks are concerned, conference trunk circuits are assigned either G711 (default) or G711 & G729OPT when selecting the codec type.

| Circuit A | | | Circuit B | | | Codec type used |
|-----------|------|---------|-----------|------|---------|-----------------|
| G711 | G729 | G729OPT | G711 | G729 | G729OPT | |
| NO | NO | NO | - | - | - | NONE |
| NO | NO | YES | - | NO | YES | G.711 |
| NO | YES | - | YES | NO | - | G.711 |
| NO | YES | - | - | NO | YES | G.729 |
| NO | YES | - | - | YES | - | G.729 |
| YES | NO | NO | YES | - | - | G.711 |
| YES | NO | YES | YES | NO | YES | G.711 |
| YES | NO | YES | YES | YES | - | G.729 |
| YES | NO | - | NO | YES | - | G.711 |
| YES | YES | - | YES | NO | YES | G.729 |
| YES | YES | - | YES | YES | - | G.729 |
| YES | - | - | YES | NO | NO | G.711 |
| - | NO | YES | NO | NO | YES | G.711 |
| - | NO | YES | NO | YES | - | G.729 |
| - | YES | - | NO | YES | - | G.729 |
| - | - | - | NO | NO | NO | NONE |

- Applies regardless of whether YES or NO is set

Table 20 Classmark handling for codec type

Generating the classmarks

The default setting is always **EC&G711&G729OPT**.

NOTE: The classmark setting in the CHANGE branches of the AMOs overwrites the setting that existed prior to the AMO call. Therefore, if an additional classmark is to be set, the existing setting must be displayed beforehand and specified again with CHANGE.

If a setting is to be reset to its default value, the value INIT must be specified.

If all classmarks are to be deactivated, the value NONE must be used.

If only some classmarks are to be deactivated, the classmark to be retained must be specified again with CHANGE. All others are automatically deleted.

Examples:

Subscriber:



Configuration Management --> Station --> Station

Click **SEARCH** and select the subscriber.



CHANGE-SDAT : STNO=54321 , TYPE=DATA1 , CLASSMRK=NONE ;
Deactivates all classmarks as required for digital data terminal devices.



CHA-SDAT : STNO=54321 , TYPE=DATA1 , CLASSMRK=EC&G711&G729 ;
Sets the EC, G711 and G729 classmarks. Use of the G.729 codec is forced if the partner has set G729 or G729OPT.



**CHANGE-
SDAT : STNO=54321 , TYPE=DATA1 , CLASSMRK=EC&G711&G729&G7290
PT&VAD ;**
Sets the classmarks for EC, G711, G729, G729OPT and VAD (in other words, all).

Attendant console:



Administration of the attendant console can only be executed in expert mode.

**Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open
...<IP> with AMO
(see AMO command)**



CHANGE-ACSU : ATNDNO=65432 , CLASSMRK=EC&G711 ;
Sets the EC and G711 classmarks. Calls are always switched without compression and the echo is suppressed.

Configuring the IPDA Feature

Configuring Subscriber, CO/Tie Trunk Circuits in Access Points

Announcement devices:

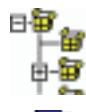
The default setting for SSC and RCSU is always **G711&G729OPT&VIAHHS&ML**. The default setting for TSCSU is **EC&G711&G729OPT&VIAHHS&ML**.

NOTE: Important note for upgrading earlier system versions
(and field trial versions)

After generation, check that the classmarks VIAHHS and ML are set. If not, set them now.

If the classmarks were not set to default, VIAHHS and ML will not be set after generation. This applies in particular to the AMO TSCSU, since the AMOs SSC and RCSU did not have any classmarks in V1.0.

NOTE: The option of setting G729OPT or even G729 for announcement devices should only be used after careful consideration. G.729 specifies a codec for **voice** compression. The codec is totally unsuitable for music compression. Music playback is extremely distorted with G.729. In some cases it may be necessary to disable G729OPT particularly if you want to avoid distortions and if circuits have been configured with codec G729.



Configuration Management --> Station --> Special Stations
Click **Search** and select the special station (**Station Type: EXTANS**).
Set or delete the required classmarks on the **Features** tab and **Save**.



ADD-SSC : PEN=1-2-37-10 , TYPE=EXTANS , CPCALL=HOLD , CLASSMRK=G711&VIAHHS&ML ;
or

CHANGE-RCSU : PEN=1-2-37-5 , CLASSMRK=G711&VIAHHS&ML ;
Disables G729OPT and sets the G711 classmark. Echo cancellation is not required at announcement devices because the path from the subscriber to the announcement device is not switched.

NOTE: The classmarks **VIAHHS** and **ML** are **enabled** by default.

They may only be disabled in exceptional cases.

In the case of **CHANGE**, do not forget to specify both classmarks if they were previously set.

If **VIAHHS** is not set, announcements and/or music on hold are no longer distributed via HHS (i.e. via the central system). Instead they are transferred directly from the HG 3575 which hosts the source to all other HG 3575 systems that require the announcement.

If **ML** is not set, an individual connection is established from the source HG 3575 for each circuit in an access point that requires an announcement or music on hold.

For further information on announcements or music on hold, refer to [Section 4.10, "External Music on Hold", on page 176](#).

Conference:

A central configuration switch is used system-wide to set whether or not compressed connections can be connected to conference units.

By default, only uncompressed RTO connections are supported with conference units. In other words, the codec classmarks associated with the conference units are set to G711.

You can use the AMO ZAND to change the setting to G711 & G729OPT.



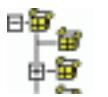
Administration of central system data can only be executed in expert mode.
Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO (see AMO command)



CHANGE-ZAND : TYPE=ALLDATA3 , IPDAVCCF=YES ;
This AMO permits compressed connections with the conference unit.

The change becomes effective immediately, that is, the next time an IP connection is connected to a conference unit.

CO/tie trunks:



Configuration Management --> System Data --> Trunk --> Trunk
Click **Search** and select the circuit.
Set or delete the classmarks for **IP connections** on the **Basic Data** tab and **Save**.



CHANGE-TACSU : PEN=1-1-91-1 , CLASSMRK=EC&G711 ;
Sets the EC and G711 classmarks. (G729OPT has effectively been deactivated in contrast to the default setting.)



CHANGE-TDCSU : PEN=1-1-91-1 , CLASSMRK=G711 ;
Sets the G711 classmark.

NOTE: If the classmark setting "NONE" is temporarily required for an outbound call (e.g. for privacy module), this can be done using an access code: AMO WABE: NOEC. This code can only be used as the prefix.

Example

Configuring the IPDA Feature

Configuring Subscriber, CO/Tie Trunk Circuits in Access Points

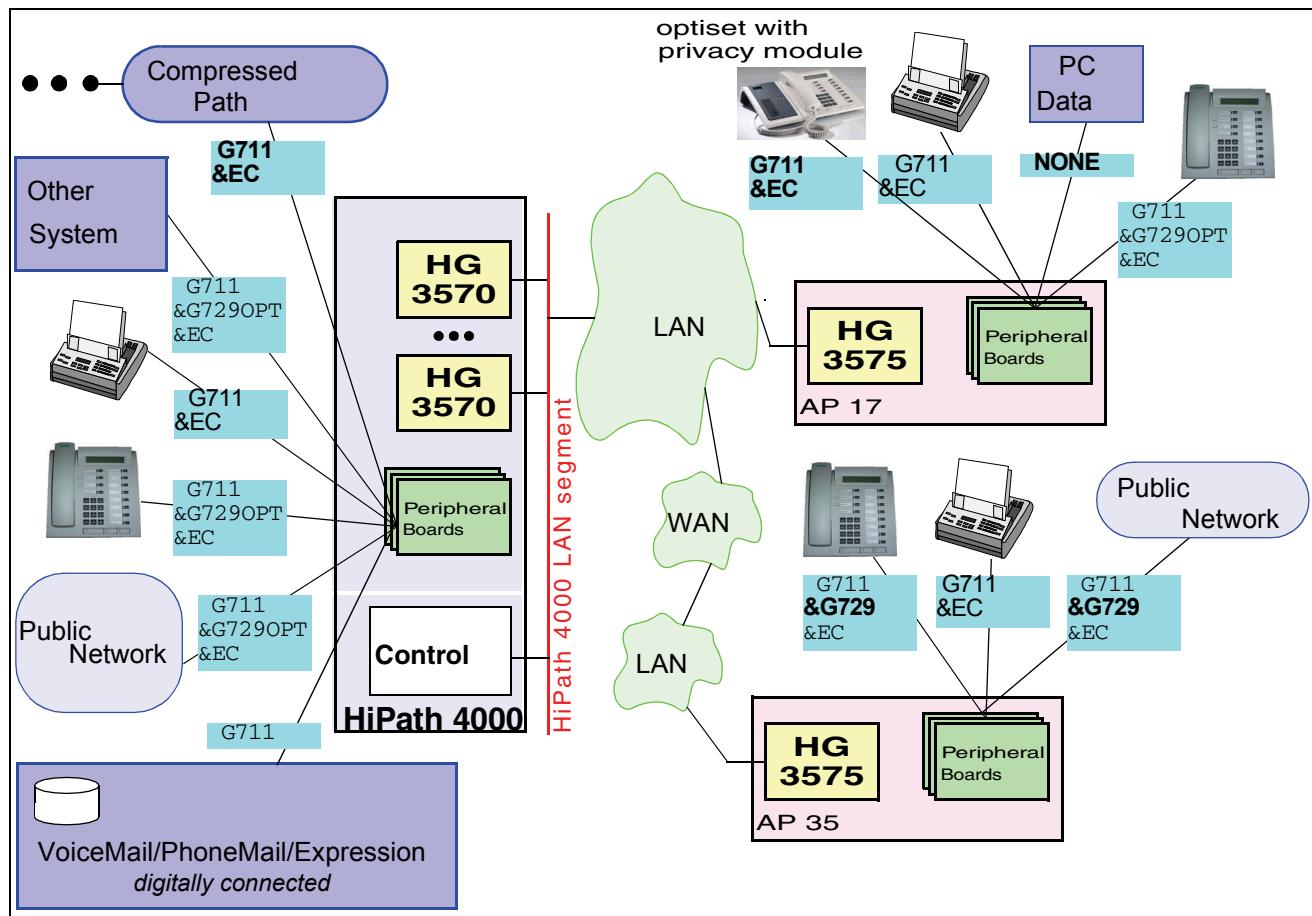


Figure 48

Classmarks

The example in [Figure 48 “Classmarks”](#) shows how classmarks are set for different circuits.

The default is G711&G729OPT&EC.

In the central system, there are three exceptions: the fax which does not tolerate signal compression, the compressed tie trunk path and the digital VoiceMail/PhoneMail/Expression server connected. Fax devices can also be configured with the default classmarks if STMI2/4 and NCUI2/4 boards are used exclusively. A sequence of compressions and expansions should be avoided. The selected G711&EC setting in the example ensures that calls from the compressed tie trunk path cannot be compressed a second time. Digital announcement/voice recording devices connected generate absolutely no echo - and save voice in compressed form. Consequently, compression is disabled and EC is deactivated.

The data terminal device on the AP 17 is set to NONE, as it tolerates neither compression nor echo cancellation or attenuation/amplification. When the ISDN service is signaled correctly in the bearer capabilities, transmission is always performed with the NONE classmark, irrespective of the classmark setting.

The Optiset with privacy module for voice encryption is configured for G711&EC. If you switch to encryption, that is, modem transmission, during a call, the gateways automatically adapt the transmission mode. The classmarks G729 or G729OPT must not be set for version 1 boards, that is, STMI/NCUI (and not STMI2/4 or NCUI2/4), because these only support automatic fax/modem recognition in uncompressed connections. This restriction does not apply to STMI2/4 and NCUI2/4 boards.

The AP 35 is connected to the central system via WAN. Bandwidth is therefore a precious commodity and voice compression should always be used if possible. The setting G711&G729&EC for telephones and the CO line ensures that calls with telephone subscribers in the central system and AP 17 are compressed, as are calls from telephones in the central system or AP 17 via the local CO line in AP 35.

Configuring the IPDA Feature

External Music on Hold

4.10 External Music on Hold

If an internal sound type (SIU) is replaced by an external sound source (e.g. music on hold), this new sound type is applied throughout the system.

In the example below ([Figure 49 “Routes for music on hold: Supply in the central system”](#)) an external MusiPhone is configured in the central system, as is most commonly the case.

IP payload connections to the central system are then required for all circuits in IPDA access points that are switched to external MOH. If multiple circuits/subscribers in one access point are connected to the same MOH, only one payload connection (B channel) is connected for transmission of music between the central system and the access point, and all relevant circuits of the AP cut in to this.

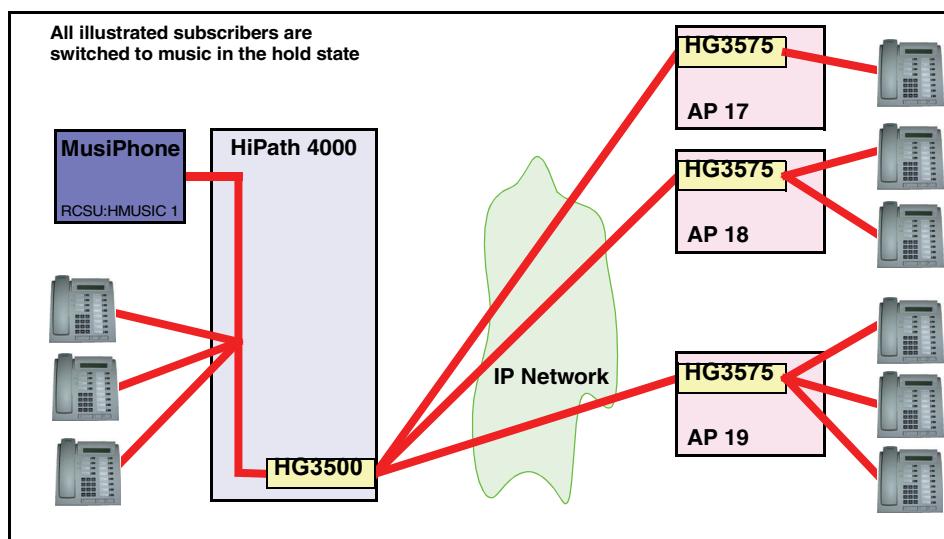


Figure 49 Routes for music on hold: Supply in the central system

NOTE: If a circuit is switched to MOH, e.g. as a result of consultation hold, the original payload connection remains active. In other words, the connection of MOH uses an additional payload connection.

If the external MOH is supplied in an access point rather than on the central system, the connections continue to be handled as explained below.

Circuits within the access point in which the MOH is supplied are switched to MOH via the internal AP memory time switch. In other words, no additional payload connections over IP are required.

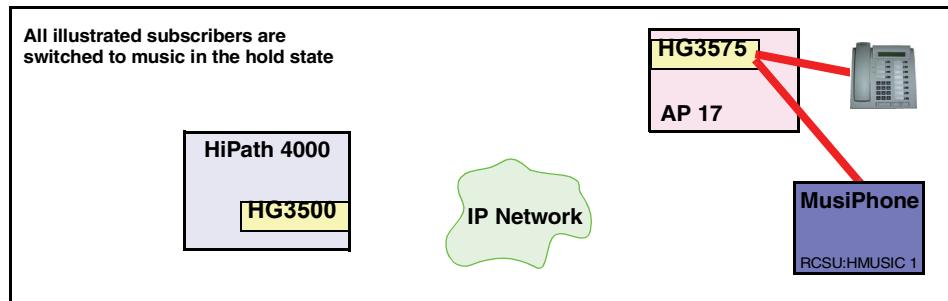


Figure 50 Routes for music on hold: Supply in access point 17 - local subscriber

If circuits in the central system are switched to MOH, a payload connection between the access point with the MOH source and the central system is switched, from which all circuits of the central system are then operated.

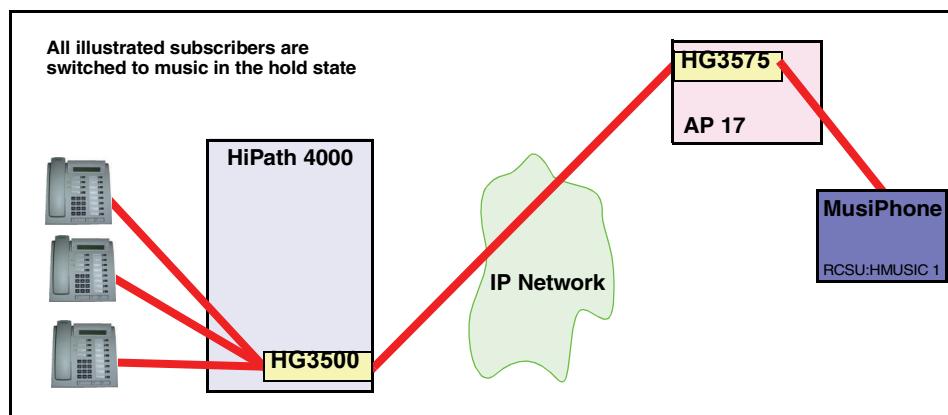


Figure 51 Routes for music on hold: Supply in access point 17 - central subscriber

If circuits of other access points are switched to MOH, a separate payload connection to the central system is switched for these access points. The central system is connected to the access point with the MOH source via a second payload connection. MOH connections between access points are therefore always switched via the central system.

There is no alternative routing via access point <-> access point connections if there are not enough or no resources available for the route via the central system.

Configuring the IPDA Feature

External Music on Hold

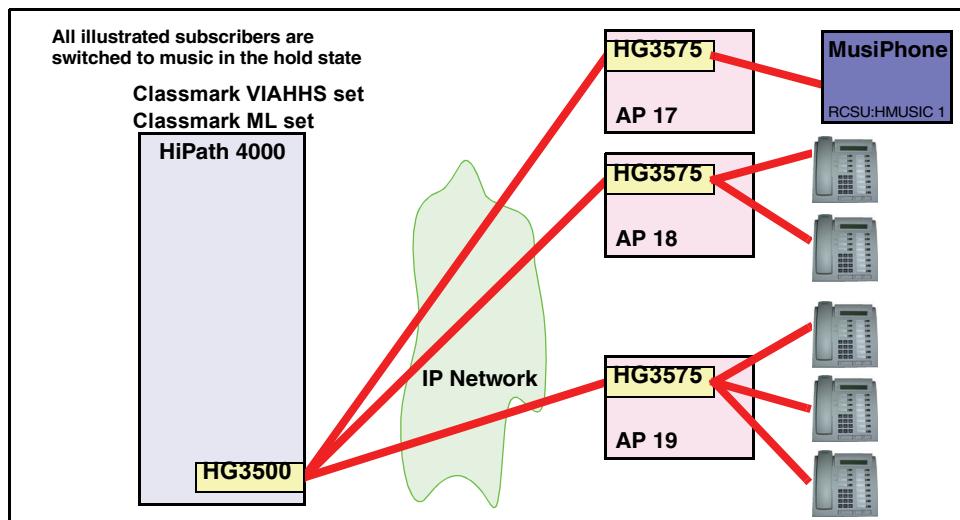


Figure 52 Routes for music on hold: Supply in access point 17 - subscriber in different AP

If the central system consists only of a HiPath 4000 V2.0 communication server without peripheral devices, MOH cannot be distributed via the central system (VIAHHS). In this case, you must disable distribution (via HiPath host system). To do this, disable the classmark VIAHHS in the classmark set of the AMOs SSC, RCSU, and TSCSU. Please note the instructions for using classmarks in Section 4.9, "Configuring Subscriber, CO/Tie Trunk Circuits in Access Points".



Configuration Management --> Station --> Special Stations
Click **Search** and select the special station (**Station Type: EXTANS**).
Set or delete the required classmarks on the **Features** tab and **Save**.



ADD-SSC : PEN=1-2-37-10 , TYPE=EXTANS , CPCALL=HOLD ,
CLASSMRK=G711&ML ;
or

CHANGE-RCSU : PEN=1-2-37-5 , CLASSMRK=G711&&ML ;

NOTE: With CHANGE, please note that you must specify all classmarks that are to be set. Classmarks that were set prior to the changes will not be taken over. Always specify the classmark **ML**, otherwise an individual payload connection to the source HG 3575 will be set up for each circuit on a HG 3575 that requires active MOH. As a result, considerable bandwidth and B channel resources are consumed.

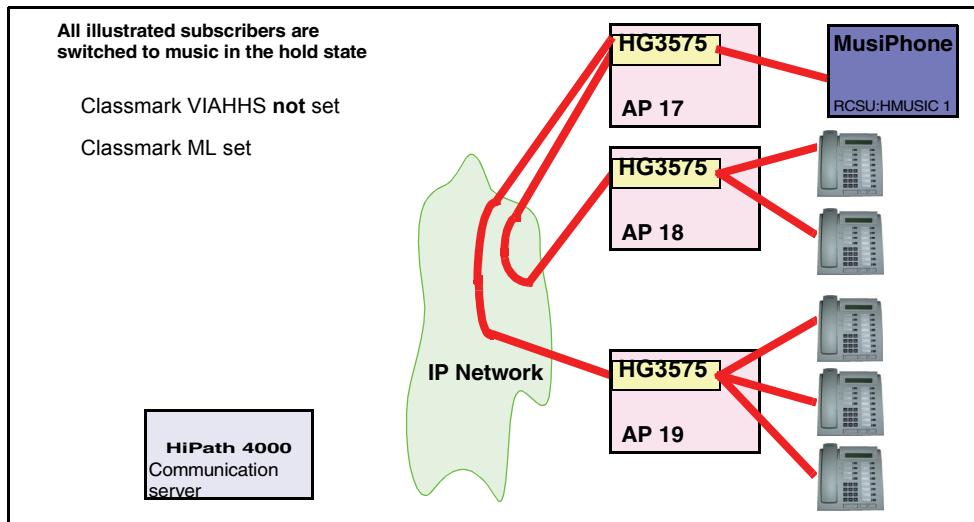


Figure 53 Routes for music on hold: Supply in access point 17 - subscriber in different AP

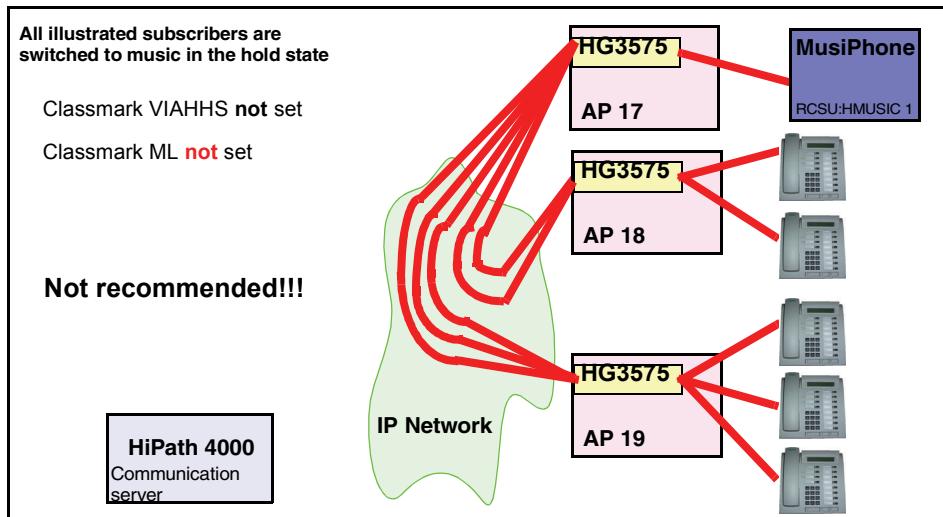


Figure 54 Routes for music on hold: Supply in access point 17 - subscriber in different AP

Multiple Music on Hold

With IPDA-based branch concepts, a requirement exists for the setting of different music on hold for different branches.

With the aid of flex routing, up to 150 different announcements can be used in the system. The announcements are assigned on a subscriber basis.

If all subscribers of an access point are assigned the same MOH and this MOH is supplied locally in the access point, no payload connections over IP are required for MOH. If, however, a subscriber is assigned MOH that is supplied in

Configuring the IPDA Feature

External Music on Hold

a different access point, two payload connections over IP are switched - one from the MOH source to the central system and one from the central system to the AP of the subscriber.

4.11 Information on CMI

The SLC16 board can be used in access points of the type AP 3300 IP. The module cannot be used in AP 3500/3505 IP and AP 3700 IP because of the SIVAPAC connector and the other screening.

Because of the IP route between the exchange and the access point, clocking is not possible between a master SLC in the exchange or an access point and slave SLC boards in their access points.

However, it is possible to configure a separate master SLC board in every access point.

SLC board clock synchronization works within an access point and thus handover works between the boards. Due to sporadic runtime problems during handover, however, it is **not permissible** to operate multiple SLC boards in a single AP.

When CMI is operated in several access points it is necessary that the DECT radio cells of the access points do **not** overlap.

If the radio cells overlap, a handset call via an SLC in access point 17 is cleared down as soon as the handset enters an AP 18 radio cell.

Handset roaming in radio cells of different access points is possible. However, note that the extension connections between the home SLC and the remote SLC could give rise to additional IP hops within a connection.

If, for example, an external call is connected via the central system to the home SLC in access point 17 (1st IP hop), but the subscriber is in the radio area of an SLC in access point 18, then an extension connection is switched between AP17 and AP18 (2nd IP hop).

The consequences are:

- Two IP hops, i.e. doubled voice delay compared to a call at AP 17.
- Two B-channel connections for one call at AP 17 (coming from the central system and going to AP 18).

These circumstances must be considered when project planning.

4.12 IP Address Changes

Unfortunately, the correct configuration of the IP addresses of all HiPath 4000 IPDA components at the time of installation is not all that is required.

Restructuring of the IP network of the customer, which also affects the addressing of the HiPath 4000 IPDA components, is part of day-to-day business.

Whenever an IP address has to be changed, there is no avoiding a brief interruption in operation. In order to minimize the effects for the users of the HiPath 4000 system, the procedure for changing addresses must be planned meticulously.

In the following scenarios, it is always assumed that the changes involved are changes that affect the entire LAN segment to which the HiPath 4000 IPDA components are connected, and not just the address of an individual component.

A distinction is made between three cases in this context:

- Change of Address in a Network Segment to which Access Points are Connected
- Changing the Address of the Survivability Network
- Changes in the HiPath 4000 LAN Segment

4.12.1 Change of Address in a Network Segment to which Access Points are Connected

Let us use the configuration of Access Point AP99 as an example:

- It is to be reached from the HiPath 4000 LAN segment via Router R_a (192.168.1.254).
- It is to reach other networks via Router R_x (192.168.23.1).
- Its own IP address is 192.168.23.99.
- The IP address for the TAP is 192.168.23.199.
- The netmask of the network in which the access point is located is 255.255.255.0

As this involves a change of the entire network segment, AP 98 is also affected with APIPADDR=192.168.23.98 and TAIPADDR=192.168.23.198.

We receive the following information from the customer's network administrator:

| Name | NEW address | OLD address |
|---------|-----------------|---------------|
| Netmask | 255.255.255.224 | 255.255.255.0 |

Table 21 *Change of address in “networked” access points*

| Name | NEW address | OLD address |
|-----------------------|---------------|----------------|
| Router R _x | 10.123.87.222 | 192.168.23.1 |
| AP 98 APIPADDR | 10.123.87.198 | 192.168.23.98 |
| AP 98 TAIPADDR | 10.123.87.208 | 192.168.23.198 |
| AP 99 APIPADDR | 10.123.87.199 | 192.168.23.99 |
| AP 99 TAIPADDR | 10.123.87.209 | 192.168.23.199 |

Table 21

Change of address in “networked” access points

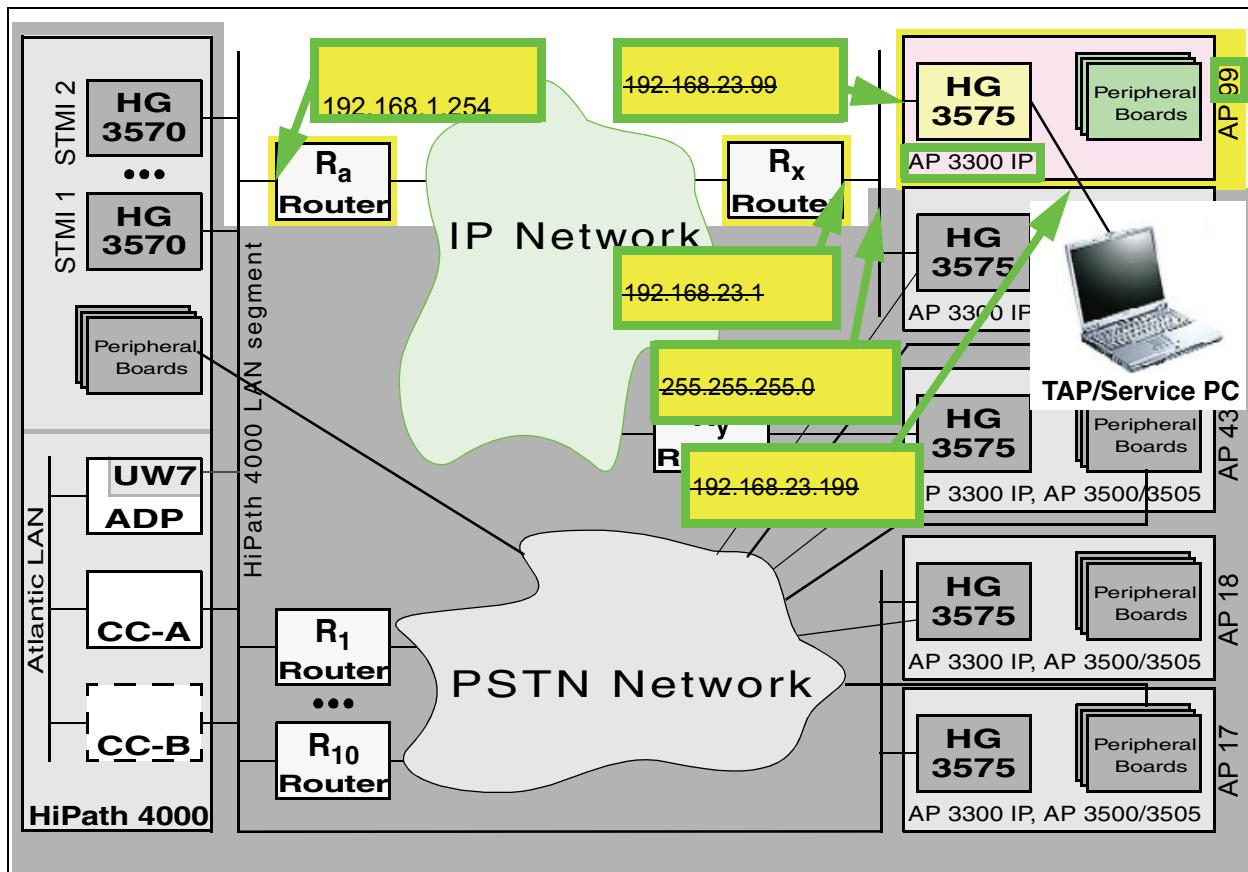


Figure 55

Change of address in “networked” access points

The time of the address change in the access points is critical.

If parallel operation of both network addressings cannot be configured in the customer network during the transition period, the address change must be oriented to the time of transition of Router R_x and the change in routing in the customer network.

Configuring the IPDA Feature

IP Address Changes

The address change must be performed prior to the reconfiguration of Router Rx and started on the access point via EXEC-USSU:UPDATAP. Existing links are disconnected. After reconfiguring the router, we would no longer be able to reach the access point and would only be able to implement the address change locally at the access point.

NOTE: Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk. Otherwise, the data on the system would conflict with the data on the HG 3575 when the system is reloaded and could only be synchronized again with EXEC-USSU:UPDATAP, LTU number, UL.

As soon as the access point has restarted with the new address, the HiPath 4000 central switch can no longer reach it via the signaling survivability route (if configured), or can only reach it via this route. This applies until the routing in the customer network has likewise been changed.

NOTE: If special routes are used in the configuration of the HiPath 4000 IPDA system (in access points or for HG 3500 modules), these must all be checked and, if necessary, modified. (CHANGE-APRT:TYPE=ROUTTBL . . .)

Generation



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.
Change the addresses on the **IP Interface** tab and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.
Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



```
CHANGE-APRT:TYPE=APNET,LTU=98,APIPADDR=10.123.87.198,  
NETMASK=255.255.255.224,TAIPADDR=10.123.87.208;  
EXEC-USSU:MODE=UPDATAP,LTU=98;  
CHANGE-APRT:TYPE=APNET,LTU=99,APIPADDR=10.123.87.199,  
NETMASK=255.255.255.224,TAIPADDR=10.123.87.209;  
EXEC-USSU:MODE=UPDATAP,LTU=99;
```

4.12.2 Changing the Address of the Survivability Network

This case scenario, while unlikely, is simple to realize in the HiPath 4000 switch. All addresses in the survivability network are fixed addresses derived from the network address.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, change the survivability network address on the **System Data** tab and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point.

Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



CHANGE-SIPCO:TYPE=LSNET , SURVNET=192.168.123.0;

The change within the access points becomes effective after

EXEC-USSU:MODE=UPDATAP , LTU=xx;
for all affected access points.

NOTE: Connections are cleared down without further warning.

Prior to the EXEC-USSU:UPDATAP, the configuration must be updated on the system hard disk.

NOTE: As ports of the survivability router are also affected by the address change, the routers also have to be reconfigured.

However, this may not be performed until after conversion of the access points.

4.12.3 Changes in the HiPath 4000 LAN Segment

This is the most complicated change of all, and the one which harbors the greatest risk, which is why address changes in the HiPath 4000 LAN segment should be avoided whenever possible.

The reason is the security concept of IPDA. An access point may only be controlled by CC-A or CC-B. To this end, the IP addresses of the two processors are configured in the access point. If these addresses change, the access point can no longer be controlled and would have to be reconfigured locally.

Configuring the IPDA Feature

IP Address Changes

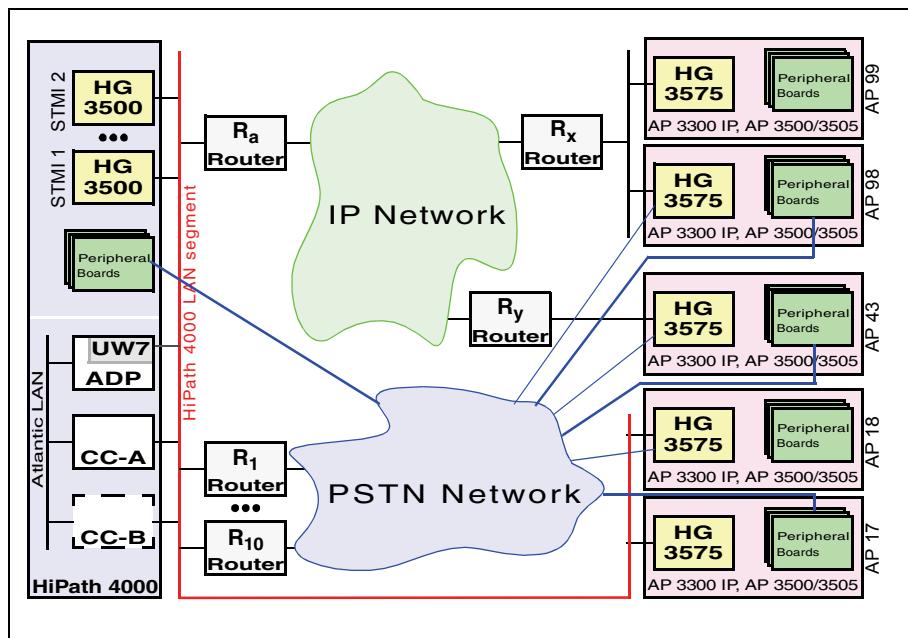


Figure 56 Installation example

We receive the following information from the customer's network administrator:

| Name | NEW address | OLD address |
|------------------------|-----------------|---------------|
| Netmask | 255.255.255.224 | 255.255.255.0 |
| Network address | 10.123.1.64 | 192.168.1.0 |
| CC-A | 10.123.1.65 | 192.168.1.1 |
| CC-B | 10.123.1.66 | 192.168.1.2 |
| ADP | 10.123.1.67 | 192.168.1.3 |
| Router R _a | 10.123.1.94 | 192.168.1.254 |
| Router R ₁ | 10.123.1.83 | 192.168.1.101 |
| Router R ₁₀ | 10.123.1.93 | 192.168.1.102 |
| AP 17 | 10.123.1.77 | 192.168.1.17 |
| AP 18 | 10.123.1.78 | 192.168.1.18 |
| STMI1 | 10.123.1.68 | 192.168.1.10 |
| STMI2 | 10.123.1.69 | 192.168.1.11 |

Table 22 Address change in HiPath 4000 LAN segment

The following procedure avoids local reconfiguration of the access points.

The changes must be implemented before the routing in the customer network is changed.

Step 1

Change the IP addresses in the HiPath 4000 LAN segment.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, change the IP addresses and, if required, **Network Mask** on the **System Data** tab and **Save**.



```
CHANGE-SIPCO:TYPE=LSNET,NETADDR=10.123.1.64,
NETMASK=255.255.255.224,DEFRT=10.123.1.94,
CCAADDR=10.123.1.65,CCBADDR=10.123.1.66;
```

This results in the addresses being changed. However, the change is not effective until the system has been restarted, which must be the last step performed in this sequence.

Step 2

The CC-A and CC-B address changes implicitly for “networked” access points. **LSRTADDR** must be explicitly modified as well as the address of the router on the HiPath 4000 LAN segment (Router R_a) used for configuring the signaling connection.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Change the address of the router in the network on the **IP Interface (NW)** tab and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



```
CHANGE-UCSU:UNIT=AP,LTU=xx,LSRTADDR=10.123.1.94;
EXEC-USSU:MODE=UPDATAP,LTU=xx;
for every "networked" AP, i.e. in this example 43, 98 and 99.
```

This puts the access points out of operation until both the CC address change in the system is effective and the routing in the customer network has been changed. Existing links are disconnected.

Step 3

Change the HiPath 4000 LAN addresses of the “direct link” access points.

It is assumed in this context that the addressing in the internal network of the “direct link” access points is not changed.

Configuring the IPDA Feature

IP Address Changes



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Change the address of the router in the network on the **IP Interface (DL)** tab and **Save**.

Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search** and select the access point. Click **Execute** on the **Action** pull-down menu and select the mode of action **Update AP**, confirm with **OK**.



```
CHANGE-UCSU:UNIT=AP,LTU=17,LSRTADDR=10.123.1.77;
```

```
EXEC-USSU:UPDATAP,17;
```

```
CHANGE-UCSU:UNIT=AP,LTU=18,LSRTADDR=10.123.1.78;
```

```
EXEC-USSU:UPDATAP,18;
```

This puts the access points out of operation until the CC address change in the system is effective. Existing links are disconnected.

Step 4

Change the survivability router addresses at the HiPath 4000 LAN segment.

In the example, this involves Routers R_1 and R_{10} . In order to change their addresses in the HiPath 4000 LAN segment, they must be deleted from the configuration and re-entered.

Unfortunately, a survivability router cannot be deleted until no more access points are configured on this router.

In this example, these are the access points 18, 43 and 98 which are configured for signaling survivability. Here, too, the configuration must be deleted and re-entered again.

The address configuration of the survivability routers (e.g. WAML) must, of course, be modified as well.

The overall procedure is as follows:

**Configuration Management --> System Data --> IPDA --> IPDA Access Point**Click **Search** and select the access point.Delete the router number on the **General** tab under **Signaling Survivability** and **Save**.**Configuration Management --> System Data --> IPDA --> IPDA Signaling Survivability Router**Click **Search** and select router --> **Delete**.Click **New**, enter router with modified data and **Save**.**Configuration Management --> System Data --> IPDA --> IPDA Access Point**Click **Search** and select the access point.Enter the router number on the **General** tab under **Signaling Survivability** and **Save**.

```
DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;
DELETE-APRT:TYPE=SURV,CONF=AP,LTU=98;
DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1;
ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,
LSADDR=10.123.1.83;
ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=1;
ADD-APRT:TYPE=SURV,CONF=AP,LTU=98,ROUTERNO=1;
```

```
DELETE-APRT:TYPE=SURV,CONF=AP,LTU=18;
DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10;
ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10,
LSADDR=10.123.1.93;
ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=10;
```

Step 5

Change the addresses of the HG 3500 modules:

**Configuration Management --> System Data --> Board --> Board**Click **Search** and select **STMI**.Change the address on the **STMI Board Data** tab under **IP Gateway** and **Save**.

```
CHA-BCSU:TYPE=IPGW,LTU=5,SLOT=85,IPADDR=10.123.1.68;
CHA-BCSU:TYPE=IPGW,LTU=5,SLOT=91,IPADDR=10.123.1.69;
```

NOTE: If special routes are used in the configuration of the HiPath 4000 IPDA system (between access points and HG 3500), these must all be checked and, if necessary, modified. (CHANGE-APRT:TYPE=ROUTTBL ...)

Configuring the IPDA Feature

IP Address Changes

Subsequently, the changed addresses have to be loaded on the HG 3500 modules via:



Configuration Management --> System Data --> Maintenance --> Board Maintenance

Click **Search** and select **STMI**.

Click **Execute** on the **Action** pull-down menu, select **Restart** and confirm with **OK**.



`RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2316-X, FCTID=1;`

Step 6

To complete the procedure, the HiPath 4000 switch now has to be reset in order for the addresses configured with SIPCO to become effective.



The restart can only be initiated in expert mode.

**Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> with AMO
(see AMO command)**



`EXEC-REST:UNIT, BP, SOFT;`

Contact with the “networked” access points cannot be re-established until the routing in the customer network has also been changed.

5 Configuring the APE Feature (Access Point Emergency)

To configure the AP Emergency feature, you must have a good understanding of the functioning of this feature. This overview is found in Chapter 2, “Access Point Emergency Feature Description”.



For emergency mode, configuration of the feature “Alternate Routing on Error“ is mostly required so that subscribers of different “emergency islands“ can contact one another.

This is described in the service manual „Feature Usage Examples“, „Alternate Routing on Error“.

In some installations trunk and tie-line circuits have to be configured in order to access a HiPath network or the public network from the “islands“.

Conclude this part of the configuration **before** configuring the AP Emergency feature.

You can prevent APE from taking effect if a fault occurs in the network for example.

If, however, the above requirements have not been fulfilled, the communication capability of an “emergency island“ may be restricted and it may no longer be possible to make emergency calls.

The feature configuration is divided into the following steps:

- Activities on HiPath 4000 central system
 - Configuring or Modifying a CC-AP in HiPath 4000
 - Configuring or Modifying an Emergency Group
 - Configuring Access Points for AP Emergency
 - Configuring the Display for AP Emergency on the optiSet/optiPoint
 - Defining the Switchover Delay
 - Time Synchronization Between the Central System and CC-AP
 - Configuring an AP Backup Server with HiPath 4000 Backup & Restore
 - Creating a Schedule for the Backup
 - Performing the First Backup
- Activities on the survivability unit - CC-AP
 - Initial Startup of the CC-AP
 - Unix Configuration on the CC-AP

Configuring the APE Feature (Access Point Emergency) *Configuring or Modifying a CC-AP in HiPath 4000*

- HiPath Backup Restore Configuration on the CC-AP
- Upgrading the AP Emergency Computer (New Fix Release/Minor Release)
- Verification and Acceptance of the AP Emergency Configuration

5.1 Configuring or Modifying a CC-AP in HiPath 4000

The CC-AP is always addressed with the LTU number of the access point in which it is integrated.

Only the IP address for the IPDA LAN connection of the CC-AP and the operating mode of the Ethernet interface are required as configuration data. All other parameters necessary for IP communication are taken from the CBM configuration of HG 3575 of the access point.

| Parameter | “Network Link“ Access Point | “Direct Link“ Access Point |
|---------------------------------------|---|--|
| IP address | | Directly configured |
| Netmask | HG 3575 network mask APRT: TYPE=APNET - NETMASK | HiPath 4000 LAN segment network mask SIPCO: TYPE=LSNET - NETMASK |
| Default router | Default router in the network of the access point UCSU: UNIT=AP - APRTADDR | Default router in the network of the access point UCSU: UNIT=AP - APRTADDR that is usually the default router of the HiPath 4000 LAN segment SIPCO: TYPE=LSNET - DEFRT |
| VLAN tagging | STMIB: MTYPE=NCUI2 - TYPE=IFDATA - VLAN | |
| VLAN ID | STMIB: MTYPE=NCUI2 - TYPE=IFDATA - VLANID | |
| TOS byte for the signaling connection | STMIB: MTYPE=NCUI2 - TYPE=IFDATA - TOSLAN | |

Table 5-1 Configuration parameters derived for the CC-AP

The Ethernet interface setting **must be identical** for both connected interface partners (CC-AP or LAN switches or routers)!

Configuring the APE Feature (Access Point Emergency)

Configuring or Modifying a CC-AP in HiPath 4000



Note: The setting of a fixed interface partner leads to problems with the "Autonegotiate" setting of the other partner.

Caution: Incorrect settings cannot normally be detected by the system and therefore go unreported. If one device is operating in full duplex and the other in half duplex mode, this is not immediately noticeable. Where there is a high payload, the device set to half duplex will report a higher number of late collisions and the packet delay will increase sharply.

If the LAN port to which the CC-AP is connected does not support auto-negotiation, or if it does not function reliably, the CC-AP Ethernet interface must be set to fixed values.

In the example, the CC-AP is configured or modified in access point 99.

The IP address is 192.168.23.199, the Ethernet interface is set to 10 Mbps, half duplex.



Configuration Management --> System Data --> IPDA --> IPDA CC Access Point
Click **Search** and select **CC-AP** or create a **New** one.

Set the **IP Address** and the Ethernet interface transmission speed (**Speed**) and mode and **Save**.



ADD-APESU:DATA=CCAP,CCAPNO=99,IPADDR=192.168.23.199,
IPDBITRT=100MBFD;
or

CHANGE-APESU:DATA=CCAP,CCAPNO=99,IPADDR=192.168.23.199,
IPDBITRT=100MBFD;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| APESU | CCAPNUM | d | LTU-Nummer des Access Points, in welchem der CC-AP eingebaut ist. |
| | CCAPNO | e | Line/Trunk Unit Number of the Access Point, where the CC-AP is installed. |
| | IPADR | d | IP Adresse des CC-AP. |
| | IPADDR | e | IP Address of the CC-AP |

Table 5-2 AMO APESU parameters in ADD or CHANGE branch under DATA=CCAP

Configuring the APE Feature (Access Point Emergency) Deleting a CC-AP in HiPath 4000

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|------------|------------------|------------------------------|---|
| | IPDBITRT | d | Einstellung der Ethernet-Schnittstelle bezüglich Bitrate und Betriebsmodus Die Einstellung beider Schnittstellenpartner (CC-AP und Port am LAN-Switch, -Router) muss identisch sein! |
| | IPDBITRT | e | Setting of Bitrate and Mode of Operation for the Ethernet Interface Both interface partners (CC-AP and port of LAN-Switch or -Router) must be set identically! |

Table 5-2 AMO APESU parameters in ADD or CHANGE branch under DATA=CCAP

5.2 Deleting a CC-AP in HiPath 4000

When you delete a CC-AP, all emergency groups allocated to it and the AP Emergency configuration of the allocated access points are also automatically deleted. If you want to keep the emergency groups, you must first allocate them to a different CC-AP (CHANGE-APESU:DATA=APEGRP, EGRPNO=xx, CCAPNO=yy;).



Configuration Management --> System Data --> IPDA --> IPDA CC Access Point
Click **Search** and select the CC-AP, then click **Delete**.



DELETE-APESU:DATA=CCAP, CCAPNO=99;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

5.3 Configuring or Modifying an Emergency Group

The emergency group is the logical connecting link between the AP and CC-AP.

An AP is a member of exactly one emergency group. An emergency group is served by exactly one CC-AP.

The emergency group was introduced for transferring complete groups of access points, together and at the same time, to and from the central system control to the CC-AP control.

While the primary function of the AP Emergency feature is handling the total breakdown of the central control, the difficulty lies in appropriate handling of partial breakdowns that may arise in the IP communication.

Configuring the APE Feature (Access Point Emergency)

Configuring or Modifying an Emergency Group

An emergency group typically combines access points that together form a survivable unit. For example, this could be external location connected via WAN.

Faults in the routing can result in only some of a group's access points losing contact with the central control. In this case it would be possible to transfer only the affected access points to the CC-AP control. This interrupts communication among the group's APs, however. Calls would then only be possible via the trunk. But does each access point have its own trunk line? Where are the central resources, such as recorded announcements, servers, etc.?

This is why it often makes sense to switch a group only as a whole. In this way all access points remain under **one** control, and communication among the access points runs via IP. All access points can communicate with the rest of the system via a common trunk line. In such cases, the access points of **one** emergency group will also belong to **one** source group for source-dependent routing (see Section 4.7, "Configuring Source Dependent Routing", on page 4-145).

An emergency group is identified by a freely selectable number. Depending on the installation, it may be advantageous to base the emergency group number on the numbering of the associated source group or the CC-AP number.

Because plain text says more than any number, no matter how cleverly selected, you can give each emergency group a name.

Each configured emergency group must be assigned to a CC-AP. The assignment can be changed.

Weighting determines whether all of an emergency group's access points switch to the CC-AP. A weighting is assigned to each access point. The access point contributes this weighting to the switching evaluation in the event of a breakdown in its connection to the central control. A limiting value can be defined for the group. When this value is exceeded, a switchover is carried out.

Because they have higher weightings, access points with trunk lines, central resources or VIP users are more likely to trigger a switchover than access points with "standard features".

When assigning the weightings, you must make sure that the weighting of all access points that are assigned to an emergency group is sufficient in order to reach the group's limiting value. This is easy to overlook, particularly when you are changing the configuration.

If the IP connections to central control are available again for all access points, switchback to central control must be organized. There will be customers who require immediate switchback to the central control, even though this means disconnecting calls. Often, however, switchback is prohibited at certain times. It may also be the case that only administrative switchovers are permitted.

AP Emergency enables the activation of either automatic switchback, or of only manual switchback. The parameters for automatic switchback are based on the level of the emergency groups.

Configuring the APE Feature (Access Point Emergency)

Configuring or Modifying an Emergency Group

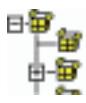
For the group - and therefore for all access points in the group - you can stipulate how long the connection between each access point and the central control must be stable without interruptions, before a switchback will be considered.

Once the connection has been stable for the specified length of time, a check is made as to whether a switchback is allowed at the time. Intervals during which a switchback is permitted are set up for this purpose. The interval starts with the specified hour (of the day) and ends at another specified hour. It is customary to set up a time offset in order to shift the network load of scheduled activities away from the exact hour. This allows you to specify how many minutes after the hour the switchback interval is opened or closed. For example, if the switchback start is at 8pm, the switchback end at 6am, and the offset is 13, this means that the switchback can automatically take place during the time from 8:13pm and 6:13am. If there was a network fault in this configuration that interrupted the IP connection between the central control and the access points from 9:05am until 9:15am, the automatic switchback would take place at 8:13pm. If the fault occurs during the switchback interval, the switchback takes place immediately once the IP connections between the central control and access points have been stable again for the minimum time.

A manual switchback is possible at any time. The administrator must ensure here that the boundary conditions are correct (is switchback required? - are all access points connected to the central control unit again?).

If a CC-AP fails while it is actively controlling access points, the following behavior results:

- If the central system is available and if it has contact with an affected AP, the central system takes control of the access point again without taking the stability time and the set switchover time into consideration.
 - This only applies if automatic switchback has been configured.
 - If manual switchback has been configured, an access point is **not** automatically taken over by the central system if the CC-AP fails during emergency mode.
- If the central system is not available, control is no longer available for the access point. It resets itself within the configured time period and waits until a control makes contact with it.



Configuration Management --> System Data --> IPDA --> AP Emergency Group

Click **Search** and select an emergency group or create a **New** one.

Set configuration parameters and **Save**.



```
ADD-APESU : DATA=APEGRP , EGRPNO=2 , CCAPNO=99 ,  
THRSHLD=100 , SBMODE= , NAME="BERLIN" ,  
STABLE=10 , SBBEGIN=20 , SBEND=6 , RSOFFSET=13 ;
```

or

```
CHANGE-APESU : DATA=APEGRP , EGRPNO=2 , CCAPNO=99 ,  
THRSHLD=100 , SBMODE=AUTO , NAME="BERLIN" ,  
STABLE=10 , SBBEGIN=20 , SBEND=6 , RSOFFSET=13 ;
```

Configuring the APE Feature (Access Point Emergency)

Configuring or Modifying an Emergency Group

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| APESU | EGRPNUM | d | Identifikations-Nummer der Emergency Gruppe. Wertebereich [1 .. 99] |
| | EGRPNO | e | Identification number of the Emergency Group. Range [1 .. 99] |
| | CCAPNUM | d | Nummer des CC-AP, dem die Emergency Gruppe zugeordnet ist. |
| | CCAPNO | e | Number of the CC-AP, to which the Emergency Group is assigned. |
| | SCHWELLE | d | Grenzwert für den Gewichtungsalgorithmus. Bei Erreichen bzw. Überschreiten werden die Access Points der Emergency Gruppe in die Steuerung des CC-AP umgeschaltet. Wertebereich [0 .. 1000] |
| | THRSHLD | e | Threshold for the weighing algorithm. When reached or exceeded, the Access Points of the Emergency Group are switched over into control of the CC-AP. Range [0 .. 1000] |
| | RSMODE | d | Rückschaltemodus Bestimmt, ob die Access Points der Emergency Gruppe automatisch, oder ausschließlich manuell zur zentralen Steuerung zurückgeschaltet werden dürfen. Werte: AUTO: Automatische Rückschaltung MAN: Manuelle Rückschaltung |
| | SBMODE | e | Switch-Back Mode Specifies if the Access Points of the Emergency Group may be switched back to the central control automatically or only manually. Values: AUTO: Automatical Switch-Back MAN: Manual Switch-Back |
| | NAME | d | Name der Emergency Gruppe (maximal 22 Zeichen) |
| | NAME | e | Name of the Emergency Group (maximum 22 characters) |

Table 5-3 AMO APESU parameters in ADD or CHANGE branch under DATA=APEGRP

Configuring the APE Feature (Access Point Emergency)
Deleting an Emergency Group

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | STABIL | d | Stabilitätszeit Minimale Zeitdauer, über welche alle Access Points der Emergency Gruppe eine stabile Verbindung zur zentralen Steuerung haben müssen, bevor automatisch rückgeschaltet werden darf. Wertebereich [0 .. 255] Minuten |
| | STABLE | e | Stability time Minimum amount of time, during which all Access Points of the Emergency Group must have a stable connection to central control, before they may be switched back. Range [0 .. 255] Minutes |
| | RSBEGIN | d | Beginn des täglichen Zeitintervalls für die automatische Rückschaltung. Die Rückschaltung ist erlaubt in der Zeit zwischen RSBEGIN:RSOFFSET und RSENDE:RSOFFSET. |
| | SBBEGIN | e | Begin of the daily time interval for the automatic switch-back. Switch-back is allowed during the time between SBBEGIN:SBOFFEST and SBEND:SBOFFEST. |
| | RSENDE | d | Ende des täglichen Zeitintervalls für die automatische Rückschaltung. Ist RSENDE gleich RSBEGIN gesetzt, darf jederzeit automatisch rückgeschaltet werden. |
| | SBEND | e | End of the daily time interval for the automatic switch-back. If SBEND is set identically to SBBEGIN, automatic switch-back is allowed at any time. |
| | RSOFFSET | d | Offsetwert [in Minuten] zum täglichen Zeitintervall für die automatische Rückschaltung. |
| | RSOFFSET | e | Offset value [in minutes] to the daily time interval for the automatic switch-back. |

Table 5-3 AMO APESU parameters in ADD or CHANGE branch under DATA=APEGRP

5.4 Deleting an Emergency Group

When you delete an emergency group, the AP Emergency configuration of the access points allocated to it are also automatically deleted. If you want to keep the configuration of the access points, you must first allocate these to a different emergency group (CHANGE-APESU:DATA=AP , APNO=xx , EGRPNO=yy ;),

Configuring the APE Feature (Access Point Emergency)

Configuring Access Points for AP Emergency



Configuration Management --> System Data --> IPDA --> AP Emergency Group
Click **Search** select CC-AP and **Delete**.



DELETE-APESU:DATA=APEGRP,EGRPNO=99;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

5.5 Configuring Access Points for AP Emergency

To configure an access point for the AP Emergency feature, it must be assigned to an already existing emergency group. Most of the configuration specific to AP Emergency is performed at the level of the emergency group.

Access points with the “direct link” connection type (APDL) - see Section 4.2, “Configuring an Access Point”, on page 4-57 - can only be assigned to emergency groups for which the CC-AP is in an access point with link type APDL.

For access points with the “networked” connection type (APNW) there is no restriction for the connection type of the access point containing the CC-AP.

You must stipulate the emergency group to which an access point belongs as well as the “weight” of the access point in question, i.e. its contribution to the weighting algorithm for the switchover.

Regardless of the weighting in the emergency group, you can also specify that an access point be immediately included in the control of the CC-AP allocated to the emergency group when the connection to the central control is lost. This exception to the group behavior can for example be useful when an access point with VIP users is equipped in such a way that it has its own trunk access and is therefore independent of the availability of the other group members.



Access points that are switched over to the CC-AP independently of the group and that do not have their own trunk or tie line only allow AP-internal communication.
This prevents emergency calls from being forwarded over the trunk, for example.

Each APs with configured ACD agents must have access to the PSTN via CO trunk. Then it is possible to divert calls from ACD agents in survivability mode.

Configuring the APE Feature (Access Point Emergency)

Configuring Access Points for AP Emergency

This exception only applies when the limiting value for the weighting within the emergency group has not been reached. The weighting contribution of an access point with separate switching is always taken into consideration for the weighting of the group behavior. The access point is always included in the switchover when required by the weighting for the emergency group. The switchback also takes place along with the group.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Set the configuration parameters in the **AP Emergency** tab and **Save**.



ADD-APESU: DATA=AP, APNO=99, EGRPNO=2, WEIGHT=70, SWMODE=GROUP;

or

CHA-APESU: DATA=AP, APNO=99, EGRPNO=2, WEIGHT=70, SWMODE=GROUP;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| APESU | APNUM | d | LTU-Nummer des Access Points |
| | APNO | e | Line/Trunk Unit Number of the Access Point |
| | EGRPNUM | d | Identifikations-Nummer der Emergency Gruppe. |
| | EGRPNO | e | Identification number of the Emergency Group. |
| | GEWICHT | d | Gewichtsbeitrag des Access Points für den Gewichtungsalgorithmus. Verliert der Access Point die Verbindung zur zentralen Steuerung, so wird sein Gewichtsbeitrag in die Gewichtung der Emergency Gruppe eingebracht. Wertebereich [0 .. 1000] |
| | WEIGHT | e | Weight share of the Access Point to the weighing algorithm. When the Access Point loses the connection with the central control, its weight share is brought into the weighing of the Emergency Group. Range [0 .. 1000] |

Table 5-4

AMO APESU parameters in ADD or CHNAGE branch under DATA=AP

Configuring the APE Feature (Access Point Emergency)

Examples for Determination of Weights

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-----|-----------|----------------------|---|
| | UMSCHALT | d | <p>Umschaltemodus Bestimmt, ob ein Access Point ausschließlich zusammen mit der gesamten Emergency Gruppe umgeschaltet wird, oder ob er auch unabhängig von der Gewichtung sofort vom CC-AP übernommen wird, wenn er die Verbindung zur zentralen Steuerung verloren hat.</p> <p>Werte: GRUPPE: Umschaltung nur mit gesamter Gruppe EINZEL: Einzelbehandlung bei der Umschaltung</p> |
| | SWMODE | e | <p>Switch-Over Mode Specifies if the Access Points may be switched over only together with the complete Emergency Group, or if it may be taken over by the CC-AP independently to the weighing, as soon as it loses connection with central control.</p> <p>Values: GROUP: Switch-Over only together with Group SINGLE: Individual handling at Switch-Over</p> |

Table 5-4 AMO APESU parameters in ADD or CHNAGE branch under DATA=AP

5.6 Examples for Determination of Weights

The combined use of access point weighting, threshold settings for group switchover and, if necessary, exemption from the group rule through individual switchover, form a powerful instrument for configuring automatic switchover to the emergency mode. The following two examples should help you to understand the calculations.

- Basic IP system (with no shelves in slots 1-15) with the communication server located at the computer center and 30 access points, 1 CC AP at the backup computer center, and multiple trunk connections with the same code distributed on four access points.

Sample configuration 1

(Emergency mode in the case of complete failure of the communication server only, i.e. the connection from **all** access points to the server has been lost)

- 1 emergency group, threshold = 300
- Weight of each of the 30 access points = 10

Disadvantage: If only one access point is not available, for example as a result of a power failure, it is excluded from the calculation since it does not have any contact with the CC AP. In such a scenario, the threshold **cannot** be reached.

Configuring the APE Feature (Access Point Emergency) *Examples for Determination of Weights*

Sample configuration 2

(If the connection between the communication server and more than half of the access points is lost, the system switches to emergency mode. This also applies if the same occurs with more than half of the trunk connections).

- 1 emergency group, threshold = 150
- Access points without a trunk connection: Weight = 10
- Access points with a trunk connection: Weight = 75
- Conventional system at main location, branch 1 with 3 access points one of which has a trunk connection; branch 2 with 6 access points, two of which have a trunk connection; branch 3 with 1 access point, which also has a trunk connection; branch 4 has 4 access points, one of which has a general trunk connection and another which contains the ports for the executive management with a separate trunk connection. Connectivity via a local trunk connection is very important for the branches. If a single access point without a trunk connection “fails”, this should not lead to a change of group. If, however, two or more access points fail, the group must be changed. Each location has an individual access point equipped with CC AP.

Sample configuration

Branch 1 (3 APs)

- 1 emergency group, threshold = 200
- Access points without a trunk connection: Weight = 100
- Access point with a trunk connection: Weight = 200

Branch 2 (6 APs)

- 1 emergency group, threshold = 200
- Access points without a trunk connection: Weight = 100
- Access points with a trunk connection: Weight = 100

Branch 3

- 1 emergency group, threshold = 100
- Access points: Weight = 100

Branch 4

- 1 emergency group, threshold = 200
- Access points without a trunk connection: Weight = 100
- Access point with a trunk connection: Weight = 200

Configuring the APE Feature (Access Point Emergency)

Removing Access Points from the AP Emergency Configuration

- Executive access point: Weight = 100, individual switchover active
The CC AP should be integrated in this access point.

5.7 Removing Access Points from the AP Emergency Configuration

You can remove an access point from the AP Emergency configuration at any time.



When you delete an access point from the AP Emergency configuration, its possible weighting contribution to the weighting algorithm of the emergency group to which it belonged is also deleted.
Verify whether the emergency group's limiting value "THRSHLD" is still a valid number.



Configuration Management --> System Data --> IPDA --> IPDA Access Point

Click **Search** and select the access point.

Delete the **Emergency Group Number** on the **AP Emergency** tab and **Save**.

DELETE-APESU:DATA=AP , APNO=99 ;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

5.8 Deleting the Entire AP Emergency Configuration

If the entire AP Emergency configuration of a HiPath 4000 system is to be deleted, this can be performed easily at system level. All CC-APs, all emergency groups and the AP Emergency configuration of all APs are completely removed.



Configuration Management --> System Data --> IPDA --> IPDA CC Access Point

Click **Search** and select the **Object list** view.

Select all (CC-AP) objects and **Delete**.

DELETE-APESU;

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

5.9 Configuring the Display for AP Emergency on the optiSet/optiPoint

If an access point is actively controlled by a survivability unit, i.e. a CC-AP, there are changes that the user needs to know about.

This information is output on the second line of the optiSet/optiPoint idle display. **The text to be output must be agreed upon with the customer.**

The output text replaces the LOGO information that can be output during normal operation.

The maximum text length is 22 characters and may comprise numbers and letters in upper and lower case.



Insert blank spaces for all positions in the second display line where information is output in idle mode, and leave enough room to allow the information to be read. For example, if the telephone's number is shown in the first 5 spaces of the idle display, you must start the AP Emergency information text with at least 6 blank spaces.

Use the AMO ZANDE for this setting.



You must be in expert mode to make this setting with the AMO ZANDE.
Expert Mode --> HiPath 4000 Expert Access --> Open ...<IP> with AMO
(see AMO command)



CHANGE-ZANDE : TYPE=ALLDATA, APEDTXT=" Emergency operation " ;
The text should be exactly 22 characters long.

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

5.10 Defining the Switchover Delay

If a breakdown has been detected in the HiPath 4000 central system or the IP network, and if a CC-IP has decided based on its configured rules that access points should be switched over, there is another point to be considered:

How should the overall system react if the HiPath 4000 central system carries out a RELOAD?

There are two possibilities:

1. React as quickly as possible, i.e. perform immediate switchover.
In the case of a RELOAD, switchover to emergency operation is then **always** performed.
2. Delay the switchover long enough to **prevent** a RELOAD leading to emergency operation.

Configuring the APE Feature (Access Point Emergency)

Defining the Switchover Delay

In line with this decision, you must set the AP Emergency switchover delay either

- to zero or
- to the length of time that the HiPath 4000 system needs to execute a complete RELOAD.



Configuration Management --> System Data --> IPDA --> IPDA System Data

Click **Search**, enter the switchover delay for AP Emergency in the **System data** and **Timing** tabs and then click **Save**.



CHANGE-SIPCO : TYPE=TIMING , APESWDLY=5 ;

Sets the switchover delay to 5 minutes

->i.e. the system RELOAD takes 5 minutes; wait for the corresponding length of time.

The modified data does not take effect until after you have used HiPath Backup Restore to copy the database to the CC-AP, and the CC-AP has accepted it.

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|---|
| SIPCO | APESWDLY | d | <p>APE Umschalteverzögerung Das Umschalten eines Access Points in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Es ist entweder Null - "schalte sofort" einzutragen, oder die Zeit, welche von der HiPath 4000 Zentrale benötigt wird, um einen RELOAD durchzuführen. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99].</p> |
| | APESWDLY | e | <p>APE Switch Over Delay The switch-over of an Access Point into Emergency Mode can be delayed for a configurable amount of time. It shall either be set to zero - "switch immediately", or to the amount of time which the central HiPath 4000 system needs to perform a RELOAD. The value is entered in minutes. Range [0 .. 99].</p> |

Table 5-5

The AP Emergency-specific parameter APESWDLY of the AMO SIPCO in CHANGE branch under TYPE=TIMING

5.11 Querying the Connection Data

5.11.1 Querying the Connection Data via Configuration Management



Configuration Management --> System Data --> Maintenance

--> IPDA - CC Access Point Maintenance

Click SEARCH and select CC-AP.

The table that this generates shows the connection status for all access points that belong to the emergency groups of the selected CC-AP.

Configuring the APE Feature (Access Point Emergency)

Querying the Connection Data

5.11.2 Querying the Connection Data via AMO



A query for the AP Emergency configuration also includes output of the current connection status. The amount of data output and the information it contains depend on the logical level at which the query is running - and whether it is performed in the HiPath 4000 central system or on a CC-AP.

DISPLAY-APESU;

- on HiPath 4000 central system
 - all CC-APs
 - all emergency groups
 - all access points
- locally on a CC-AP
 - local CC-AP
 - all of the CC-AP Emergency groups
 - all access points of the CC-AP Emergency groups

DISPLAY-APESU:CCAPNO=xx; or DISPLAY-APESU:xx;

- on HiPath 4000 central system
 - selected CC-AP
 - all of the selected CC-AP Emergency groups
 - all access points of the selected CC-AP Emergency groups
- locally on a CC-AP
 - if the local CC-AP is selected
 - local CC-AP
 - all of the CC-AP Emergency groups
 - all access points of the CC-AP Emergency groups
 - if the local CC-AP is not selected: system message

DISPLAY-APESU:EGRPNO=xx; or DISPLAY-APESU:,xx;

- HiPath 4000 central system

Configuring the APE Feature (Access Point Emergency) Querying the Connection Data

- selected emergency group
- all access points in the selected emergency group
- locally on a CC-AP
 - if an emergency group in the local CC-AP is selected
 - selected emergency group
 - all access points in the selected emergency group
 - otherwise: system message

DISPLAY-APESU:APNO=xx; or DISPLAY-APESU:, ,xx;

- HiPath 4000 central system
 - selected access point
- locally on a CC-AP
 - if an access point of an emergency group in the local CC-AP is selected
 - selected access point
 - otherwise: system message

CC-AP-specific block:

```
+-----+
| CC-AP: 99                               IP ADDRESS: 192.168.23 .199
| SPEED/WORK MODE(IPDA): 100MBFD
+-----+
```

Emergency group-specific block:

```
+-----+
| AP EMERGENCY GROUP: 2      CC-AP: 99          NAME: BERLIN
| THRSHLD: 100             SBMODE: AUTO
| STABLE: 10   MIN         SBBEGIN: 20 H       SBEND: 6   H     SBOFFSET: 13 MIN
+-----+
```

Access point-specific block:

```
+-----+
| AP: 99  AP EMERGENCY GROUP: 2  CC-AP: 99  WEIGHT: 70      SWMODE: GROUP
| CONTROL UNIT: HOST-CC        SIGNAL PATH: LAN
| LAST RECORDED CONNECTION STATUS CHANGE:
|
|     HOST-CC: CONNECTED: yes    CONNECTED SINCE: 08-06-2004 18:20
|     CC-AP:   CONNECTED: yes    CONNECTED SINCE: 18-06-2004 23:01
+-----+
```

Configuring the APE Feature (Access Point Emergency)

Administration Switchover of APs

5.12 Administration Switchover of APs

5.12.1 Administration Switchover of APs via Configuration Management



Configuration Management --> System Data --> Maintenance --> IPDA - CC Access Point Maintenance

Click **Search** and select CC-AP.

In the main menu, select -> **Action -> Execute.**

In the mask that this generates, you can set

- whether the switchover should be to normal or emergency mode,
- whether a particular AP, all APs of a particular emergency group, all APs of all emergency groups in the selected CC-AP, or the entire system should be switched over.

5.12.2 Administrator Switchover of APs via AMO



Administrative switchover of access points to and from the central control to CC-AP is possible at any time.

The task is forwarded to the HiPath central system via AMO. From there, it is sent to the affected CC-AP via an affected access point. Finally, the CC-AP instructs the HG 3575 of the affected access points to start up with the requested control (central control (host) or CC-AP). If more than one CC-AP is affected, this process is repeated for each CC-AP.

Communication from the HiPath 4000 central system to the CC-AP via access points requires that at least one access point has a connection to both the central control and the CC-AP. If this is not the case, switchover cannot be initiated.

The switchover can take place at various levels:

- all access points of all emergency groups of all CC-APs in the system

EXEC-APESU: SYSMODE=EMERG, LEVEL=SYSTEM;
switches to the CC-AP

EXEC-APESU: SYSMODE=NORMAL, LEVEL=SYSTEM;
switches to the central control

- all access points of all emergency groups of one CC-AP

Configuring the APE Feature (Access Point Emergency) *Administration Switchover of APs*

EXEC-APESU : SYSMODE=EMERG , LEVEL=CCAP , NO=99 ;
switches to the CC-AP

EXEC-APESU : SYSMODE=NORMAL , LEVEL=CCAP , NO=99 ;
switches to the central control

- all access points of one emergency group (of one CC-AP)

EXEC-APESU : SYSMODE=EMERG , LEVEL=APEGRP , NO=2 ;
switches to the CC-AP

EXEC-APESU : SYSMODE=NORMAL , LEVEL=APEGRP , NO=2 ;
switches to the central control

- one access point (of one emergency group (of one CC-AP))

EXEC-APESU : SYSMODE=EMERG , LEVEL=AP , NO=99 ;
switches to CC-AP

EXEC-APESU : SYSMODE=NORMAL , LEVEL=AP , NO=99 ;
switches to the central control



The switchover is always performed for all selected access points that have contact with the requested control, regardless of group rules.

If some access points in a selection (SYSTEM, CC-AP, APEGRP) do not have contact with the requested control, these are **not** switched over.

The AMO then issues the message “partially performed”.

Following a partial switchover, resources important for operation (such as trunk lines) may not be available for a group!

For this reason, the connection status **must** be queried and verified before a manual switchover. See Section 5.11, “Querying the Connection Data”, on page 5-207.



Access points that are switched over independently of the group and that do not have their own trunk or tie line only allow AP-internal communication.

This prevents emergency calls from being forwarded over the trunk, for example.

Configuring the APE Feature (Access Point Emergency)

Time Synchronization Between the Central System and CC-AP

| AMO | Parameter | Sprache/ Language | Beschreibung/ Description |
|-------|-----------|----------------------|--|
| APESU | SYSMODE | d | Gibt an, welche Steuerung übernehmen soll. Werte: NORMAL: zentrale Steuerung (Host) EMERG: Emergency Steuerung (CC-AP) |
| | SYSMODE | e | Identifies, which control shall take over. Values: NORMAL: Central Control (Host) EMERG: Emergency Control (CC-AP) |
| | LEVEL | d | Gibt an, auf welcher System-Ebene umgeschaltet werden soll. Werte: SYSTEM: gesamtes System (alle APs, APEGRPs, CC-APs) CCAP: ein CC-AP (alle APs, APEGRPs) APEGRP: eine Emergency Gruppe (alle APs) AP: ein Access Point |
| | LEVEL | e | Identifies on which system level the switch over shall be executed. Values: SYSTEM: complete system (all APs, APEGRPs, CC-APs) CCAP: one CC-AP (all APs, APEGRPs) APEGRP: one Emergency Group (alle APs) AP: one Access Point |
| | NUMMER | d | Gibt die Nummer des betroffenen CC-AP, der Emergency Gruppe oder des AP an. |
| | NO | e | Identifies the number of the affected CC-AP, Emergency Group or Access Point |

Table 5-6 AMO APESU parameter in the EXEC branch

5.13 Time Synchronization Between the Central System and CC-AP

An exact time is required for many HiPath 4000 functions. Up until now there was only one clock per system, but with AP Emergency there are up to 84 clocks in the system and they have to operate synchronously. Time is synchronized via the Unix system. It is configured using the Unix Basic Administration system.

There are two options:

Configuring the APE Feature (Access Point Emergency) *Time Synchronization Between the Central System and CC-AP*

1. A time server is available in the IP network, which supports time synchronization of all HiPath 4000 processors (ADP and all CC-APs) using the network time protocol.
2. A time server is **not** available in the IP network. The HiPath 4000 central system must make its time available to all CC-APs via the network for synchronization purposes.

Configuring Time Synchronization using UBA

Preparation

- Use the web browser to go to the HiPath 4000 Assistant home page on the central system and log on using the ID “engr”.
- In the left menu bar, select the function area **Base Administration**.
- As the submenu option of **Base Administration**, select the application **Unix Base Administration**.
- In the UNIX Basic Administration user interface, select the function **Date/Time** under “System Administration”.

1. NTP Server in the Network

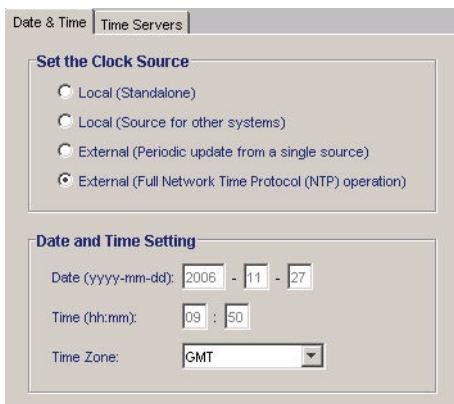


Figure 5-1 Time Server Settings for Central System / with NTP - Date & Time tab

Configuring the APE Feature (Access Point Emergency) Time Synchronization Between the Central System and CC-AP

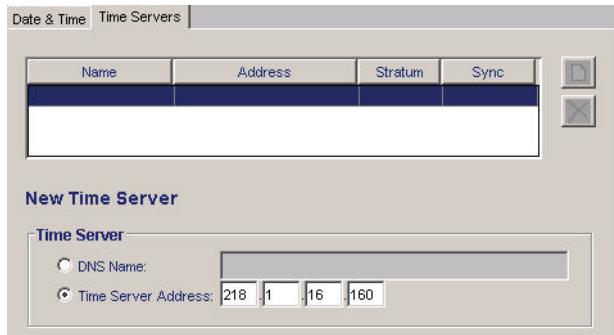


Figure 5-2 Time Server Settings for Central System / with NTP - Time Servers tab

- You must ensure that the HiPath 4000 central system is synchronized in the network for time servers.
- Select the **Date & Time** page. Check whether or not the item **External (Full NTP (Network Time Protocol) Mode)** has been set in the **Set the Clock Source** section.
- If it has not been set, NTP mode will have to be configured. To do this, you will need the host name or the IP address of the time server.
- If necessary, correct the setting of the time zone in the **Date and Time Setting** section.
- Now switch to the **Time Servers** page and - if a time server has not been configured - create at least one new time server.
- Click the icon
- Identify the time server under its DNS (host) name (**DNS Name**) or by means of its IP address (**Time Server Address**).



You can only enter a host name if either it is configured directly in UBA or if the name resolution is configured with DNS!

- Complete the input by clicking **Add**.
 - Switch back to the **Date & Time** page and conclude the procedure by clicking **Modify**.
2. HiPath 4000 Central System as Time Server

Configuring the APE Feature (Access Point Emergency) Time Synchronization Between the Central System and CC-AP

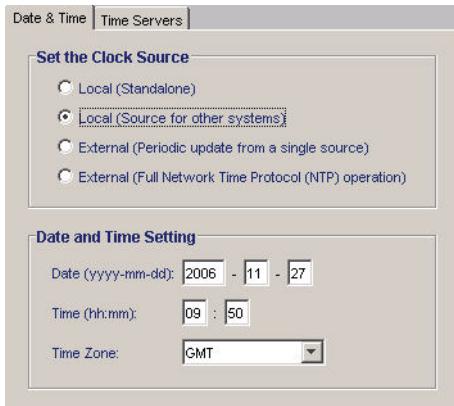


Figure 5-3 Time Server Settings for Central System / without NTP - Date & Time tab

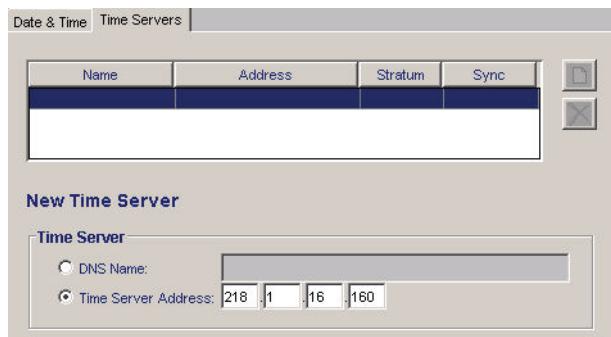


Figure 5-4 Time Server Settings for Central System / without NTP - Time Servers tab

- Select the **Date & Time** page. Select the item **Local (Source for Other Systems)** in the **Set the Clock Source** section.
- If necessary, correct the setting of the date, time and time zone in the **Date and Time Setting** section.
- Complete the changes by clicking **Modify**.

Configuring the APE Feature (Access Point Emergency)

HiPath 4000 Backup & Restore

5.14 HiPath 4000 Backup & Restore

To support the backup and restore processes for the AP Emergency feature, the HiPath Backup & Restore (HBR) application replicates the software (including RMX and Unix updates) and the configuration data from the central system to the CC-APs.

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 (partially) - only the parts of the Unix software needed on the CC-AP.
The Unix configuration data is **not** included in the backup set.

To include all software (including patches) and configuration data, the backup type “AP Emergency” and the archive type “AP Backup Server“ have been defined.

Backup type “AP Emergency“

Backup type “AP Emergency“ contains the following data:

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

The Unix configuration data is **not** included in the type APE backup sets.

Archive type “AP Backup Server“

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



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

The type “AP backup server“ archive can only contain one “AP Emergency“ type backup set. Other types of backup sets (data, system or logical) are not permitted.

The HBR of each CC-AP scans a configured and activated AP backup server every 10 minutes, as long as the CC-AP is not in emergency mode (it does not actively control any access points). If a new completed backup is found and if this backup has not been blocked by another CC-AP, 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 AP backup server.

Basic conditions regarding timing

A backup can only be carried out when the AP backup server is free, i.e. not currently blocked by restore processes. You can set the number of simultaneous restore processes allowed, in order to limit the load on the server or network.

The interval between two scheduled backups must therefore be sufficient to allow the backup and restore processes of all CC-APs in the system to be carried out.

If the number of CC-APs is larger than the number of restore operations supported simultaneously, some CC-APs must wait until the capacity on the AP backup server is free before performing restore procedures. This leads to an increase in the required restore time that must be considered in the process as a whole.

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.

If the restore process on the CC-AP requires a great deal of time (available transmission bandwidth is limited), you must ensure that all CC-APs can be restored at the same time.

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.

5.14.1 Configuring an AP Backup Server with HiPath 4000 Backup & Restore

In the first configuration step, you define where the HiPath 4000 backup data should be stored. To do this, you must specify the computer that should act as the file server (AP backup server), the directory where the data should be stored, and the login data for access. Configuration on the file server (create the directory, define the user ID) should be completed before the configuration as part of HiPath Backup & Restore.

Configuring the APE Feature (Access Point Emergency)

HiPath 4000 Backup & Restore

So that the software and data replication to the HiPath 4000 can be configured, the central system Unix must be completely configured via UBA.

- Use the Web browser to display the HiPath 4000 Assistant start page and log in with the user ID “rstas”.
- In the left menu bar, select the function area **Software Management**.
- Select the application **Backup & Restore** provided as a submenu option under **Software Management**.
- In the HiPath 4000 Backup & Restore user interface, select the function **AP Backup Server** under **Administration**.

Administration Backup AP Server

Protocol: NFS FTP
10 Maximal number of concurrent CC-AP transfers

IP Address: 218.1.16.160 Login: apeftp

(Don't use IP Address together with Host Name) (For security reasons use apeftp as login. For details see Service Documentation, section Complex Solutions, Configuring the APE Feature.)

Host Name: Password:

Directory: /AS/BACKUP/IPDA Account:

Additional Information:

110: Customer Backup Server not configured.

Figure 5-5 HBR: configuring an AP backup server

The following fields must be now be completed:

- Select the **Protocol (FTP or NFS)** - typically: **FTP**

If you want to configure the AP backup server on the HiPath 4000 central system, you must select FTP as the protocol.

- **Maximum number of concurrent CC-AP transfers**

In the maximum configuration, 83 CC-APs may want to sign on to the AP backup server and download the latest backup set simultaneously. If the server does not support this large number of simultaneously logged-in systems, or if you want to reduce possible load peaks on the server, you can adjust the maximum number of simultaneously logged-in CC-APs accordingly. Dependencies are shown in “Section 5.14, “Basic conditions regarding timing”, on page 5-217“.

- Enter the **IP Address** or **Host Name** of the AP backup server
You can only enter a host name if either it is configured directly in UBA or if the name resolution is configured with DNS.
- Enter the **Directory** on the AP backup server that should be used for the backup and restore
If you want to configure the AP backup server on the HiPath 4000 central system, you must select the directory already provided for this purpose (“/.AS/BACKUP/IPDA”).
The directory must be able to hold approximately 100 MB of data.
- If you selected **FTP** as the protocol, you still need to configure the **Login** name and the **Password** for accessing the AP backup server (FTP server). If the FTP server requires an **Account**, this also needs to be entered.
If you want to run the AP backup server on the HiPath 4000 central system, for security reasons you should configure the login under “apeftp”. You do not need to configure an account in this case.



Remember that the login password for the AP backup server must be maintained, both on the backup server and in the HBR configuration of the HiPath 4000 central system and the CC-APs.

Complete the AP backup server configuration with

- **Testing** - Save the configuration and test the access to the AP backup server.
You should always use this option if the file server is already available when it is configured in the network.
- **Configure** - Save the configuration without an access test.
You should only use this option if the file server is not available when it is configured in the network.

In this way, memory is configured for the backup.

5.14.2 Creating a Schedule for the Backup

In the second configuration step, you must now define when HiPath Backup & Restore should carry out a backup on the configured AP backup server. Typically, a backup is performed daily at a time when there is not much activity.

Configuring the APE Feature (Access Point Emergency)

HiPath 4000 Backup & Restore

When you select a start time for the backup, keep in mind that this also indirectly defines the start time for the restore on the CC-APs. The restore on the CC-AP starts as soon as the CC-AP detects availability of new completed backup. Dependencies are shown in the section "Section 5.14, "Basic conditions regarding timing", on page 5-217".

Prerequisite:

- Logged on to the HiPath 4000 Assistant via a Web browser under the ID "rsta".
- **Software Management -> Backup & Restore** has been started.
- In the HiPath Backup & Restore user interface, select the function **Schedule**.

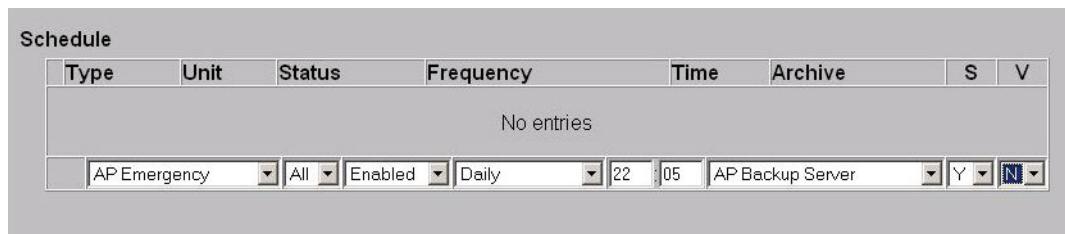


Figure 5-6 HBR: Creating a schedule for the backup

The following fields must be now be completed:

| Field name | Value | Explanation |
|------------|---|---|
| Type | AP Emergency | Only this value is permitted |
| Unit | All | Only this value is permitted |
| Status | Activated | This is where a configured schedule can be activated or deactivated. |
| Frequency | Daily (weekdays, Mondays, Tuesdays, Wednesdays, ...) | Typically, a backup should be carried out daily. |
| Time | Hour: Minute | Time of day at which the backup should start |
| Archive | AP backup server | Only this value is permitted - AP backup server must already have been configured. |
| S | Yes | Synchronize before backup, i.e. perform UPDATE. Must be set to Yes so that the latest version of the database is saved. |
| V | Yes/No | Backup data verification |

Table 5-7 Input fields in the HBR schedule

To perform more than one backup a day, enter additional daily backups in the schedule, for example, one backup at 12 noon and an additional one at 6pm.

Complete the AP backup server configuration with

- **Add New-** The new entry is saved in the timetable. A backup is performed according to the configuration.

This completes configuration on the HiPath 4000 central system.

The time required for a backup procedure depends heavily on the amount of data to be transferred and the transmission bandwidth available between the central system and the AP backup server. The procedure takes at least one hour.

5.14.3 Performing the First Backup

So that as little time as possible is lost before the CC-APs can collect the data, it may be useful to initiate a backup immediately, i.e. outside of the configured schedule.

Do this by selecting a schedule for AP Emergency and clicking **Start now**.

The first system backup takes the longest, because all saved data (approximately 100 MB) must be transferred to the AP backup server for the first time. The time required is also heavily dependent on the available bandwidth in the IP network between the HiPath 4000 central system and the AP backup server.

5.14.4 Using HBR For More Extensive Changes in the System

If you need to make extensive changes to the system, or if you are importing a new system version, the following requirements could arise:

- Larger configuration changes should be distributed to all CC-APs as quickly as possible
 - After completing the changes, you should initiate an “unscheduled” backup. However, make sure that you verify that there is sufficient transmission bandwidth available in the network at this time to complete the backup and the subsequent restore operations of the CC-APs. Remember that you cannot cancel backup and restore procedures that are active.

It may be useful to deactivate the backup process before making the changes. -> See the second point.

In the HBR, go to the schedule for the backup type “AP Emergency” and click **Start now**. It is not advisable to use “Backup” for this. If you do, you must remember to run an EXEC-UPDAT beforehand.

- You should verify new SW (regardless of whether it is a pre-revision bug fix of an LW or a new system version) on the central system first, before distributing it to all CC-APs.

Configuring the APE Feature (Access Point Emergency)

HiPath 4000 Backup & Restore

- *Before importing new SW:*

In the HBR, go to the schedule for the backup type “AP Emergency“ and change the status from “**activated**“ to “**deactivated**“. If there are several entries in the schedule for the backup type “AP Emergency“, you must deactivate all entries that could apply during the planned interval.

- *After successful verification of the SW:*

In the HBR, go to the schedule for the backup type “AP Emergency“ and change the status from “**deactivated**“ back to “**activated**“. If there are several entries in the schedule for the backup type “AP Emergency“, you must activate all entries that you previously deactivated.

If the network allows it, it may be useful to initiate an unscheduled backup. -> See the first point.

5.14.5 Checking the Regular Activities of HBR

In addition to the “usual“ methods (log files etc.), there is an option for communication with the backup server to query when and which processor was last in contact with the AP backup server.

Prerequisite:

- Logged on to the HiPath 4000 Assistant via a Web browser under the ID “rsta“.
- **Software Management -> HiPath Backup & Restore** has been started.
- In the HiPath Backup & Restore user interface, select the function **Log Files** .

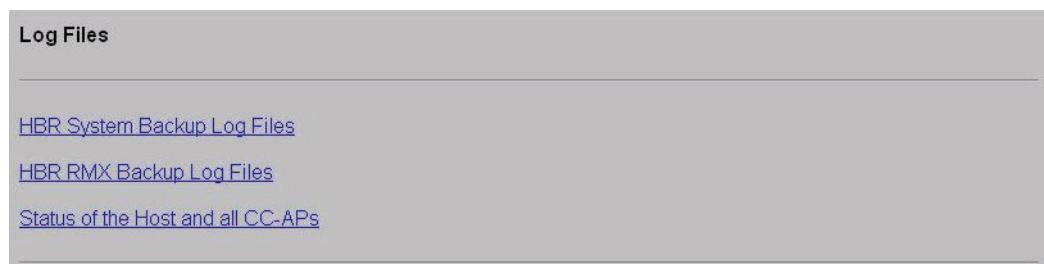


Figure 5-7 HBR - Select “Log Files“

- Select “Status of Host and All CC-APs“ from the list

Configuring the APE Feature (Access Point Emergency) *Initial Startup of the CC-AP*

Status of the Host and all CC-APs:

| Name | Status | Date/Time | Activity | Log |
|-----------|--------|---------------------|----------|-----|
| Host | OK | 2004-10-12 11:01:29 | - | - |
| CC-AP(18) | OK | 2004-10-12 17:58:10 | - | - |

Figure 5-8 HBR - Status of Host and CC-APs

The date and time data must be interpreted as follows:

- Host: Conclusion of last backup procedure
CC-AP: Time of last query on AP backup server
(normally queries once every 10 minutes)

5.15 Initial Startup of the CC-AP

The CC-AP is delivered with an empty hard disk. For the initial startup of a CC-AP, you will need a prepared MO disk/HDCF, from which the DSCXL processor starts up as the ADP. The MO disk/HDCF must have "mother hard disk" status in the system's program system and must feature the software package for the initial Unix installation.



To operate a CC AP, you will require a DSCXL board (release E1 or later).

5.15.1 Part Number of the Current APS on the HiPath 4000 Central System

During the initial installation, you must make sure that the same APS version that is currently running on the central system is copied to the CC-AP hard disk. This is particularly important for the Unix section because it does not support a "downgrade" to older versions.



DISPLAY-APS;

This display on the HiPath 4000 central system outputs the part numbers of the loaded program system. Of interest here is the part number of the Y0-APS.

PROGRAM SYSTEM : Y0-EN0YC

VERSION NUMBER : 10

Configuring the APE Feature (Access Point Emergency)

Initial Startup of the CC-AP

CORRECTION VERSION NUMBER : 001

PART NUMBER : **P30252xxxxxxxxxxxx**

PROGRAM SYSTEM WITH CODE SUBSYSTEMS

INTERFACE VERSION:

PROGRAM SYSTEM CONTAINS NO INTERFACE VERSION

5.15.2 Creating an MO Disk / HDCF for the First Startup of the CC-AP

MO-Disk

Prerequisite: PC with access to SW distribution server and MO drive.

Load the entire program system with the located part number from the SW distribution server to the PC.

- Link to entry into SWS: https://huzd309b.be001.siemens.net/en/p_nav1.html
- Find the necessary program system under “Communication System“, “HiPath 4000“, “HiPath 4000 V2.0“.
- Download the “RMX“ program system, ZIP file (just under 500 MB) and the UNIX OSBASE (approx. 100 MB).
- Unpack the contents of the ZIP file onto the PC’s local hard disk.
- Use PCHI to generate an MO disk for the initial startup.

HDCF

Prerequisite: HDCF is empty

A bootable HDCF (with the content of the chosen HiPath 4000 mother HD) must be created in a HHS (cPCI system) with COPY-DDRSM.

COPY-DDRSM:A1,1,E&I,6,E&I;

For more information, refer to "Implementation Scenarios for Features > Using HDCF instead of HDMO".

5.15.3 Starting the CC-AP

Insert the prepared MO disk into the CC-AP’s MO drive or insert the HDCF board and start the CC-AP by connecting it to a suitable power supply (either 110-230 V AC or 48 V DC, depending on the power supply unit). The processor starts up as an ADP.



At this point, the CC-AP should not yet be connected to the customer network! This means that you should not connect any LAN cable to the “CUSTOMER” and “IPDA” ports on the DSCXL board.

Set up a LAN connection between the service PC (LCT) and the DSCXL. Use the LAN port on the DSCXL that is marked “SERVICE”. Configure the LAN interface of the service PC at the IP address, e.g. 192.0.2.19. Start ComWin.

5.15.4 Copying the Program System from the MO Disk/HDCF to the Hard Disk



The hard disk must be empty before you carry out the copy procedure.
This requirement is met by new hard disks when they are delivered.
If this requirement is not fulfilled, you must boot from the MO disk/HDCF by pressing the LCT key and subsequently the RES key on the DSCXL board.

Enter the following AMO command in ComWin:



```
CHANGE-DSSM:A1,1;  
DEACTIVATE-DSSM:A1,1;  
START-INIT:A1,A1H11;  
COPY-DDRSM:A1,6,E&I,1,E&I;
```

The copy procedure takes approximately 20 minutes.

5.15.5 Reloading the CC-AP - Initial Unix Installation

- Connect the service PC's serial interface (LCT) via a V.24 zero modem cable to the serial SERVICE interface of the DSCXL board.
- On the service PC, start HyperTerminal or a comparable terminal emulation program. Set the interface to 38400 Bps, 8 data bits, no parity, 1 stop bit.
- Perform a reload of the CC-AP from the hard disk.
(EXEC-REST: SYSTEM, RELOAD;)
- After the reload, the system will start up and begin the initial Unix installation. This takes about two hours.

Configuring the APE Feature (Access Point Emergency)

Initial Startup of the CC-AP



If the hard disk memory was not empty before initial installation and a Unix system was already installed, you must reinstall the Unix.

To do this, you must activate the boot menu in the terminal emulation by pressing the Escape key within two seconds of startup.

```
ADP BIOS          (C) Fri Sep 12 10:30:55 MET DST 2003 siemens AG  
Code seg base : 579F000  
Data seg base : 57C8000
```

PCI service directory copied.

Press '**ESC**' to activate the menu

In the first menu select the entry

"1) Unix functions"

and in the subsequent menu select

"1) Install and activate UNIX from RMX :SCR: area (first inst.)"

The Unix will now install itself before installing the Unix applications.

- Do not carry out any further actions on the CC-AP until you see the message " Activation of 'First Installation' was successful" on the terminal emulation.



The following two advisory messages are always displayed when the Unix is booted. These messages can be ignored.

"server unix: WARNING: pci: Unknown PCI access mechanism! ..."

Unix cannot access the PCI bus

"server unix: WARNING: eeE80 Slot 0 - Trying once to regain link by resetting the PHY ..."

At this point, you cannot activate an Ethernet link to the customer LAN as there is no connection.

5.15.6 RMX Configuration of the CC-AP

You must now configure the number to be used for addressing the CC-AP. This is the LTU number of the access point AP 3700 IP in which the CC-AP is installed.

You must first make a few basic settings regarding the architecture. These settings will later be automatically overwritten with the central system data.

Configuring the APE Feature (Access Point Emergency) *Initial Startup of the CC-AP*



```
EXEC-DBC : ARCH=4000 , ARCHTYPE=1 ;
EXEC-APC ;
CHANGE-DATE : YEAR=#### , MONTH=## , DAY=## , HOUR=## , MINUTE=## ,
SECOND=## ;
```

After completing the RMX configuration, i.e. when the CC-AP computer has been configured, only DBC, APC and DATE can still be displayed. However, an EXEC or CHANGE is also no longer necessary.

```
CHANGE-CPCI : TYPE=SYSCONF , MONO=YES , RTM=NO , OEM=NO ;
EXEC-UPDAT :A1 , ALL ;
EXEC-REST :SYSTEM , RELOAD ;
```

```
ADD-APESM : LTU number ;
EXEC-UPDAT :A1 , ALL ;
EXEC-REST :SYSTEM , RELOAD ;
```

It will take about five minutes to reboot Unix after the RELOADS.

5.15.7 Unix Configuration on the CC-AP

Prerequisite: A LAN connection between the service PC (LCT) and the DSCXL “SERVICE” LAN port. IP address of the service PC, such as 192.0.2.19.



At this point, the CC-AP should not yet be connected to the customer network! This means that you should not connect any LAN cable to the “CUSTOMER” and “IPDA” ports on the DSCXL board.

- Start the Internet Explorer on the service PC and open the URL “<https://192.0.2.5>“.
- Log on as “engr“. During this first log on, you will be prompted to assign a password for this user ID.
- In the left menu bar, select the function area **Base Administration**.
- As the submenu option of **Base Administration**, select the application **Unix Base Administration**.

5.15.7.1 Configuring the IP Address in the CUSTOMER Network

- In the UNIX Base Administration user interface, select the function **LAN Cards** under “LAN Configuration“.

Configuring the APE Feature (Access Point Emergency)

Initial Startup of the CC-AP



- Activate the entry in the list and click the icon to select changing the **LAN card properties**.
The display shows the current setting, which was predefined during the installation:
Address. 192.1.2.5, network mask 255.255.255.0, broadcast 192.1.2.255.
- Now change these values to the data that was agreed upon with the customer for this CC-AP. The broadcast address is updated automatically when you click this field after entering the address and network mask.
- Complete the changes by clicking “Modify”.

5.15.7.2 Configuring the Default Router

- Next, in the left menu bar, select the function **Routes**.
- Click the icon to create a new route.
- Enter the data in the “Route Properties“ area.
 - Activate the “Def.“ selection for configuring the default route.
 - Under “Gateway“, enter the default router’s IP address for the UNIX part of the CC-AP. You can obtain this address from the network administrator of the customer network.
 - Under metrics, configure the maximum number of IP hops for a CC-AP connection in the customer network. The value is available from the network administrator of the customer network.

Additional settings in the UNIX Basic Administration may be necessary in certain cases. Consult the Unix Basic Administration Manual for further information.

- In the left menu bar, under **System Administration**, next select the **Shut Down** function. This starts the CC-AP and activates the new address settings.

5.15.7.3 Configuring Time Synchronization

The time of the CC-AP must run in synch with the clock in the central system. Time is synchronized via the Unix system. It is configured using the Unix Basic Administration system.

There are two options:

- A time server is available in the IP network, which supports time synchronization of all HiPath 4000 processors (ADP and all CC-APs) using the network time protocol.
- A time server is **not** available in the IP network. The HiPath 4000 central system makes its time available to all CC-APs via the network for synchronization purposes.

Preparation

Configuring the APE Feature (Access Point Emergency) *Initial Startup of the CC-AP*

- In the UNIX Basic Administration user interface, select the function **Date/Time** under “System Administration”.
1. NTP Server in the Network

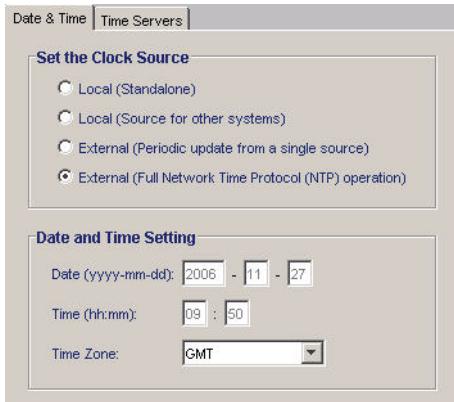


Figure 5-9 Time Server Setting for CC-AP / with NTP - Date & Time tab

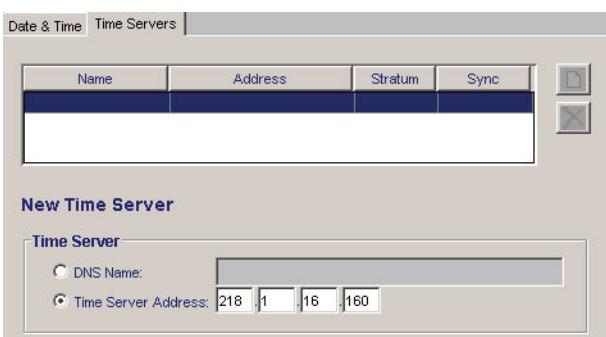


Figure 5-10 Time Server Setting for CC-AP / with NTP - Time Servers tab

- Select the **Date & Time** page. Set the item **External (Full NTP (Network Time Protocol) Mode)** in the **Set the Clock Source** section.
- If necessary, correct the setting of the time zone in the **Date and Time Setting** section.
- Now switch to the **Time Servers** page and create at least one new time server.
- Click the icon 
- Identify the time server under its DNS (host) name (**DNS Name**) or by means of its IP address (**Time Server Address**).



You can only enter a host name if either it is configured directly in UBA or if the name resolution is configured with DNS!

Configuring the APE Feature (Access Point Emergency)

Initial Startup of the CC-AP

- Complete the input by clicking **Add**.
 - Switch back to the **Date & Time** page and conclude the procedure by clicking **Modify**.
2. HiPath 4000 Central System as Time Server

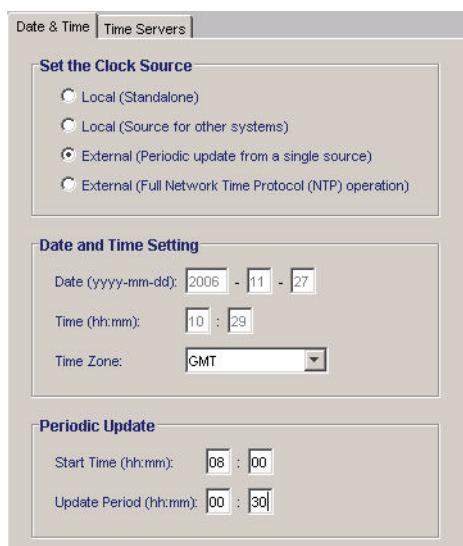


Figure 5-11 Time Server Setting for CC-AP / without NTP - Date & Time tab

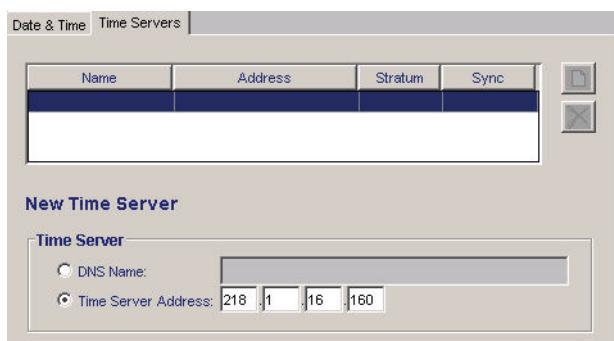


Figure 5-12 Time Server Setting for CC-AP / without NTP - Time Servers tab

- Select the **Date & Time** page. Set the item **External (periodic synchronization with a single source)** in the **Set the Clock Source** section.
- If necessary, correct the setting of the time zone in the **Date and Time Setting** section.
- In the **Periodic Update** section, specify the time at which synchronization should start (hour:minute) and the interval at which synchronization should then be repeated (hours:minutes).

Configuring the APE Feature (Access Point Emergency) *Initial Startup of the CC-AP*

- Now switch to the **Time Servers** page and create a new HiPath 4000 central system as the time server.

- Click the icon 

- Identify the HiPath 4000 by means of its IP address (**Time Server Address**) or its DNS (host) name (**DNS Name**) in the customer network. You can only enter a host name if either it is configured directly in UBA or if the name resolution is configured with DNS.
- Complete the input by clicking **Add**.
- Switch back to the **Date & Time** page and conclude the procedure by clicking **Modify**.

Additional settings in the **Unix Basic Administration** may be necessary in certain cases. Consult the Unix Basic Administration Manual for further information.



The Unix settings on the central system are not applied on the CC AP. Firewall settings for RMX access by applications (e.g. CAP) via the Unix customer LAN interface must be directly configured in the CC AP.

- In the left menu bar, under **System Administration**, next select the **Shut Down** function. This starts the CC-AP and activates the new address settings.

Configuring the APE Feature (Access Point Emergency)

HiPath Backup Restore Configuration on the CC-AP

5.16 HiPath Backup Restore Configuration on the CC-AP

5.16.1 Preparation

After completing Unix Basic Administration (Section 5.15.7, “Unix Configuration on the CC-AP”, on page 5-227), you can connect the "CUSTOMER" LAN port on the DSCXL to the customer network. This also makes it possible for Backup & Restore to access the backup server. You can now connect the IPDA port on the DSCXL with the customer network.

A LAN connection between the service PC (LCT) and the DSCXL “SERVICE“ LAN port. IP address of the service PC, such as 192.0.2.19.

5.16.2 Generating the GLA

After completing the basic configuration, you must generate the “Golden Load Area“ on the basis of this configuration.

- Start the Internet Explorer on the service PC and open the URL “<https://xxx.xxx.xxx.xxx>“, where the x's represent the DSCXL's configured IP address.
- Use the Web browser to display the HiPath 4000 Assistant start page and log in with the user ID “rstas“.
- In the left menu bar, select the function area **Software Management**.
- Select the application **HiPath Backup & Restore** provided as a submenu option under **Software Management**.
- In the **Backup & Restore** user interface, select the function **GLA/PDS**.
- Select the items **Copy HD-PDS -> GLA** and **Option RMX-UPDATE**.
- Click **Start now** and wait for the copy procedure to finish (approximately 15 minutes).

Configuring the APE Feature (Access Point Emergency) *HiPath Backup Restore Configuration on the CC-AP*



Figure 5-13 Generating the GLA on the CC-AP

5.16.3 Configuring the AP Backup Server on the CC-AP

For the automatic restore of the saved data, you must stipulate where the HiPath 4000 backup data should be retrieved. This requires that you set up the computer, directory and login data exactly as they were for the AP backup server on the HiPath 4000 central system (see Section 5.14.1, “Configuring an AP Backup Server with HiPath 4000 Backup & Restore”, on page 5-217).

- In the HiPath Backup & Restore user interface, select the function **AP Backup Server** under **Administration**.

Configuring the APE Feature (Access Point Emergency)

HiPath Backup Restore Configuration on the CC-AP

The screenshot shows the 'Administration Backup AP Server' configuration page for the CC-AP (18). The 'Protocol' field has 'FTP' selected. The 'IP Address' field contains '218.1.16.160'. The 'Login' field is set to 'apeftp'. There is a note: '(For security reasons use apeftp as login. For details see Service Documentation, section Complex Solutions, Configuring the APE Feature.)'. The 'Host Name' field is empty. The 'Directory' field contains '/AS/BACKUP/IPDA'. The 'Password' field is redacted. The 'Account' field is empty. An 'Additional Information' section is present at the bottom.

Figure 5-14 HBR: Configuring an AP backup server on the CC-AP

You must now complete the following fields with the same settings as the HiPath 4000 central system:

- **Protocol** (FTP or NFS) - typically: FTP.
- **IP Address** or **Host Name** of the AP backup server.
- **Directories** on the AP backup server.
- If you selected **FTP** as the protocol, you still need to configure the **Login** name and the **Password** for accessing the AP backup server (FTP server). If the FTP server requires an **Account**, this also needs to be entered.



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

- By activating **Automatic restore disabled**, you can deactivate the restore process. Activate this switch only temporarily and never forget to deactivate the switch for routine operation.

Complete the AP backup server configuration with

- **Testing** - Save the configuration and test the access to the AP backup server.

This option tests whether the installation works, i.e.

- whether the connection to the AP backup server can be established.

Configuring the APE Feature (Access Point Emergency) *HiPath Backup Restore Configuration on the CC-AP*

- Login with the configured data is possible
- Access to the configured directory is possible
- **Configure** - Save the configuration without an access test.

Use this option only when it is still not possible to establish a connection to the “CUSTOMER” LAN.

Make sure that you test the settings once a connection to the “CUSTOMER” LAN is possible.

Access to the AP backup server has now been configured. The HiPath 4000 Backup & Restore application on the CC-AP will now immediately start to contact the AP backup server every 10 minutes, check whether a new, completed backup set is available, and download and activate the modified sections of the backup set.



Before the first restore, HBR performs a complete backup on the hard disk. This backup is used as a reference for determining modified files that must be retrieved from the AP backup server when the system is restored. You do have to initiate the backup manually. In addition, you cannot prevent it. This procedure takes approximately one hour.

The time required for the restore procedure depends heavily on the amount of data to be transferred and the transmission bandwidth available between the AP backup server and the CC-AP. The procedure takes at least a half hour.

5.16.4 Configuring a Routine Configuration Data Backup to Hard Disk

While the CC-AP draws the essential configuration data from the central system using restore, a regular backup of the specific local CC-AP configuration is still worthwhile. Because changes to the local configuration are rather rare, a weekly backup is sufficient. When defining the starting time, make sure that this backup should run at an appropriate time, i.e. after the central system backup and subsequent restore on the CC-AP.

The example is based on the following plan:

- Start backup of the central system: daily at 10:05pm
- Completion of the CC-AP restore: by 6:30am, at the latest
- Local backup to hard disk: Sundays at 12:05pm

Prerequisite for the configuration:

- Logged on to the HiPath 4000 Assistant via a Web browser under the ID “rsta”.
- **Software Management -> Backup & Restore** has been started.
- In the HiPath Backup & Restore user interface, select the function **Schedule**.

Configuring the APE Feature (Access Point Emergency)

HiPath Backup Restore Configuration on the CC-AP

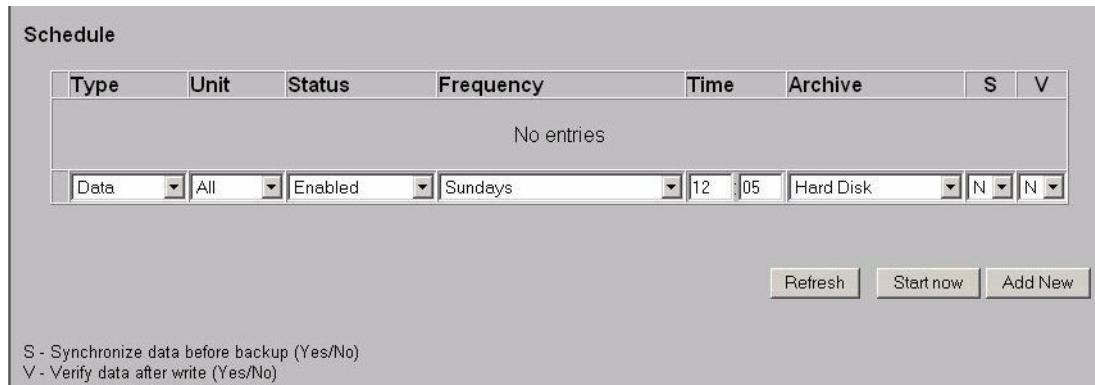


Figure 5-15 HBR: Creating a schedule for the configuration data backup

The following fields must be completed:

| Field name | Value | Explanation |
|------------|----------------------|--|
| Type | Data | Only this value is permitted |
| Unit | All | Only this value is permitted |
| status | Activated | This is where a configured schedule can be activated or deactivated. |
| Frequency | for example, Sundays | Typically, a backup should be carried out weekly, for example, on Sundays. |
| Time | Hour: Minute | Time of day at which the backup should start |
| Archive | Hard disk | Only this value is permitted |
| S | Yes/No | Synchronize before backup, i.e. perform UPDATE. - Is not necessary in this case. |
| V | Yes/No | Backup data verification |

Table 5-8 Schedule input fields for the configuration data backup

Complete setup of the configuration data backup with

- **Add New** - The new entry is saved in the schedule. A backup is performed according to the configuration.

A backup procedure takes approx. 10 minutes.

5.16.5 Creating a Routine Backup on MO Disk/HDCF

To enable generation of an operational CC-AP as quickly as possible in the event of a hard disk fault, a routine backup to an MO disk/HDCF should be performed.

Prerequisite for the configuration:

- Logged on to the HiPath 4000 Assistant via a Web browser under the ID “rsta”.
- **Software Management -> HiPath Backup & Restore** has been started.
- In the HiPath Backup & Restore user interface, select the function **Schedule**.

The backup to the MO disk/HDCF should be performed with the backup of the configuration data. It should also be performed once a week. You can set the start time to 15 minutes after the start of the configuration data backup.

Schedule

| Type | Unit | Status | Frequency | Time | Archive | S | V |
|------------|------|---------|-----------|-------|---------|---|---|
| No entries | | | | | | | |
| mo-rmx | All | Enabled | Sundays | 12:20 | MO-RMX | N | N |

S - Synchronize data before backup (Yes/No)
 V - Verify data after write (Yes/No)

Figure 5-16 HBR: Creating a schedule for the backup to MO disk / HDCF

The following fields must be now be completed:

| Field name | Value | Explanation |
|------------|----------------------|--|
| Type | mo-rmx | Only this value is permitted |
| Unit | All | Only this value is permitted |
| status | Activated | This is where a configured schedule can be activated or deactivated. |
| Frequency | for example, Sundays | Typically, a backup should be carried out weekly, for example, on Sundays. |
| Time | Hour: Minute | Time of day at which the backup should start |
| Archive | MO-RMX | Only this value is permitted. |

Table 5-9 Input fields for the schedule for the backup to MO disk

Configuring the APE Feature (Access Point Emergency)

HiPath Backup Restore Configuration on the CC-AP

| Field name | Value | Explanation |
|------------|--------|--|
| S | Yes/No | Synchronize before backup, i.e. perform UPDATE. - Is not necessary in this case. |
| V | Yes/No | Backup data verification |

Table 5-9 Input fields for the schedule for the backup to MO disk

Complete the AP backup server configuration with

- **Add New** - The new entry is saved in the schedule. A backup is performed according to the configuration.

Make sure that an MO disk is always inserted in the CC-AP MO drive for the backup.

5.17 Upgrading the AP Emergency Computer (New Fix Release/Minor Release)

Procedure

The AP emergency computer regularly checks its backup sector for updated software packages. If there is a new software package there, it is copied to the AP emergency computer.

Notes

- If an RMX upgrade was performed via SWT2/SWA (Hotfix/FixRelease/MinorRelease upgrade), then the RMX & UW7 software is upgraded in APE following the backup/restore.
- If an RMX upgrade was performed by replacing the HD within the context of the same major release, then the APE integrates both the RMX software and the UW7 software. This function is not guaranteed for a software upgrade to a future major release.
- If an RMX upgrade was performed by replacing the HD (major release switch), then the procedure is the same as a new installation and the APE integrates only the RMX software. The UW7 software is not upgraded.
- **The APE functionality is not dependent on the UW7 version and therefore guaranteed accordingly.**

5.18 Verification and Acceptance of the AP Emergency Configuration

The customer uses the AP Emergency feature to facilitate telephone calls during emergency situations where the central control and/or essential components of the IP infrastructure are not available.

As a rule, this emergency situation occurs only very rarely. For this reason it is particularly crucial that the emergency measures function as intended, should they actually be needed at some point.

It is essential that the function of the AP Emergency configuration be verified by an acceptance test after the initial startup and after substantial modifications.

To this end, each emergency group must be switched over once to the CC-AP for administration. In emergency operation, it must then be verified that emergency calls, communication to the trunk and other systems in the network, and communication between emergency groups at different CC-APs function as planned. Where applicable, also include installed applications that support emergency operation in the test.

Also verify the communications capability of access points that can be switched to the CC-AP independently of the emergency group when the group is running in normal operation.

You can conduct the tests when the system load is low.

Configuring the APE Feature (Access Point Emergency)

Verification and Acceptance of the AP Emergency Configuration

6 Load Calculation

The following bit rate calculations only take one direction into account. The route back in the opposite direction requires the same bit rate.

If a “shared medium“ is used for both directions, i.e. both directions are routed via the same line, then both directions also have to be included in the calculation.

This is the case with 10Base5, 10Base2 and 10BaseT or 100BaseT half-duplex.

The Ethernet Media Access Layer (MAC) is realized pursuant to the IEEE 802.3 / DIX Ethernet II Standard with MAC-Type 0800 (IP) in the case of the HiPath 4000 IPDA components. The alternative pursuant to IEEE 802.3 and 802.2 LLC/SNAP is not customary and would require greater bandwidth.

The calculations have been performed with active VLAN Tagging pursuant to IEEE 802.1q. This yields the higher network load. Without VLAN Tagging, the packet size is reduced by 4 octets (bytes).



Note:

The bit rate calculation used in this manual differs from that used in previous versions.

By popular demand, the bit rate is no longer specified on the Physical Layer (PHY), but instead on the Media Access Layer (MAC).

The 8 bytes for the preamble are no longer included in the calculation.

Payload transport with RTP (Realtime Transmission Protocol)

| Codec type | Sample size [ms] | Payload [Octets] | Ethernet packet size [Octets] | Ratio Overhead / Payload | Ethernet load No preamble [Kbps] | Ratio RTP / ISDN bit rate |
|---------------|------------------|------------------|-------------------------------|--------------------------|----------------------------------|---------------------------|
| G.711 | 20 | 160 | 222 | 39% | 88.8 | 139% |
| G.711 | 30 | 240 | 302 | 26% | 80.5 | 126% |
| G.711 | 60 | 480 | 542 | 13% | 72.3 | 113% |
| G.729A | 20 | 20 | 82 | 310% | 32.8 | 51% |
| G.729A | 40 | 40 | 102 | 155% | 20.4 | 32% |
| G.729A | 60 | 60 | 122 | 103% | 16.3 | 25% |

Table 6-1 Load calculation for an RTP connection (VoIP)

Load Calculation

The G.711 codec generates a sample every 125 µs.

The G.729A codec generates a 10-octet frame every 10 ms.

The overhead calculation is based on the following:

| Protocol | Overhead |
|---|-----------|
| RTP | 12 |
| UDP | 8 |
| IP | 20 |
| IEEE 802.1Q VLAN Tagging | 4 |
| Ethernet MAC (DA,SA,TYPE,FCS - no preamble) | 18 |
| Total | 62 |

Table 6-2 Overhead with RTP connections

The transmission bit rate depends not only on the codec type used and the sample size, but also on the stack layer on which the bit rate is calculated. Details on configuring the RTP payload can be found in Section 6.3, “Calculation Basis - Configuring Payload Packets”.

In this document, the “worst case“ on the physical layer is always considered, i.e. the Ethernet MAC frame including FCS with activated VLAN tagging. The bit rates on higher stack layers are also important when calculating the load following implementation on other media. The table below provides an overview. The values are specified in Kbps and apply to an RTP connection in one direction:

| Stack layer (Protocol) | Codec type / Sample size | | | | | |
|--|--------------------------|-------|-------|-------|-------|-------|
| | G.711 | | | G.729 | | |
| | 20 ms | 30 ms | 60 ms | 20 ms | 30 ms | 60 ms |
| RTP | 68.8 | 67.2 | 65.6 | 12.8 | 10.4 | 9.6 |
| UDP | 72.0 | 69.3 | 66.7 | 16.0 | 12.0 | 10.7 |
| IP | 80.0 | 74.7 | 69.3 | 24.0 | 16.0 | 13.3 |
| Ethernet No preamble No VLAN TAG | 84.0 | 79.5 | 71.7 | 31.2 | 19.6 | 15.7 |
| Ethernet No preamble With VLAN TAG | 85.6 | 80.5 | 72.3 | 32.8 | 20.4 | 16.3 |

Table 6-3 Load for an RTP connection [Kbps]- by stack layer

| | | | | | | |
|--|------|------|------|------|------|------|
| Ethernet With preamble No VLAN TAG | 87.2 | 81.6 | 72.8 | 34.4 | 21.2 | 16.8 |
| Ethernet With preamble With VLAN TAG | 88.8 | 82.7 | 73.3 | 36.0 | 22.0 | 17.3 |

Table 6-3 Load for an RTP connection [Kbps]- by stack layer

RTP load during inactivity of VAD or DMC master connections

If “idle” is detected when Voice Activity Detection has been enabled, audio signals will not be transmitted temporarily. Nonetheless, the load on the RTP connection does not drop completely to zero because data continues to be transmitted on the RTP connection to check the connection and (depending on the codec) to transmit the background noise. This data is referred to as SID frames (**Silence Insertion Descriptor**). The RTCP connection is not affected by VAD.

| Stack Layer (Protocol) | Codec Type | |
|--|------------|-------|
| | G.711 | G.729 |
| RTP | 1.8 | 1.1 |
| UDP | 2.5 | 1.8 |
| IP | 4.1 | 3.4 |
| Ethernet, No preamble, No VLAN TAG | 4.9 | 4.2 |
| Ethernet, No preamble, With VLAN TAG | 5.2 | 4.5 |
| Ethernet, With preamble, No VLAN TAG | 5.5 | 4.8 |
| Ethernet, With preamble, With VLAN TAG | 5.8 | 5.1 |

Table 6-4 Load on an RTP connection [kbps] with VAD during inactivity

The payload connection is controlled via the parallel RTCP connection (Realtime Transmission Control Protocol)

A **Sender Report** message is sent by each relevant connection partner every five seconds for every RTP connection. No Receiver Reports are sent. This produces a load of 0.2 Kbps in each direction. The packet size was once again calculated with VLAN tag and preamble.

Load Calculation

| Report type | Report interval [s] | Average Ethernet packet size [Octets] | Ethernet load excl. preamble [Kbps] |
|---------------|------------------------|---|---|
| Sender report | 5 | 130 | 0.2 |

Table 6-5 Load calculation for an RTCP connection

6.1 Load Calculation for Access Points

Calculation of the high-priority load for an individual access point

| Protocol | Data type | Maximum bit rate/ port [Kbps] | Total bit rate [Kbps] with N payload ports | | |
|-------------------|---|-------------------------------------|---|--------------|---------------|
| | | | N=30 | N=60 | N=120 |
| RTP | VoIP | 88.8 | 2,664 | 5,328 | 10,656 |
| RTCP | VoIP | 0.2 | 6 | 12 | 25 |
| TCP/IP | Signaling | 64.0 | 64 | 64 | 64 |
| TCP/IP | Supervisory (only if signaling supervisory is configured) | 0.1 | 4 | 8 | 15 |
| Total load | | | 2,738 | 5,412 | 10,760 |

Table 6-6 High-priority load of an access point (G.711/20 ms sample size)

The requisite bit rate for a supervisory connection depends on the configuration of the keep-alive timer for this connection. The parameter to this end is SUPVTIME in the TIMING branch of the AMO SIPCO. The maximum values are specified in the table.

The load which is generated through signaling and control between the HiPath 4000 central system and an access point - which is also a high-priority load - has been specified globally as 64 Kbps.

However, the actual load depends on the number of subscriber lines, CO and tie trunks and the actual telephone usage behavior in the access point.

If, however, modules are reloaded, additional load is generated which, in the case of limited bandwidth, can delay the signaling.

The absolute minimum of signaling bandwidth required is 32 kbps. If less than 64 kbps signaling bandwidth is available, traffic shaping must be enabled and set to the actual bandwidth available. See Section 4.6.1, “Restriction of the Available Signaling Bandwidth (Traffic Shaping)”, on page 4-132.

In addition to high-priority load, low-priority load portions may also arise in certain situations for the following:

- SNMP queries via network management
- TAP/Service PC access at the access point
- FTP-loading of a new HG 3575 loadware as a background task

Load Calculation

Load Calculation for Access Points

High-priority load of an access point as a function of codec type and sample size

| Codec type | Sample size | RTP load [Kbps] with N payload ports | | | Total Ethernet load [Kbps] with N payload ports | | |
|---------------|-------------|--------------------------------------|--------------|--------------|---|--------------|--------------|
| | | N=30 | N=60 | N=120 | N=30 | N=60 | N=120 |
| G.711 | 20 | 2,664 | 5,328 | 10,656 | 2,738 | 5,412 | 10,760 |
| G.711 | 30 | 2,416 | 4,832 | 9,664 | 2,490 | 4,916 | 9,768 |
| G.711 | 60 | 2,168 | 4,336 | 8,672 | 2,242 | 4,420 | 8,776 |
| G.729A | 20 | 984 | 1,968 | 3,936 | 1,058 | 2,052 | 4,040 |
| G.729A | 40 | 612 | 1,224 | 2,448 | 686 | 1,308 | 2,552 |
| G.729A | 60 | 488 | 976 | 1,952 | 562 | 1,060 | 2,056 |

Table 6-7 High-priority load of an AP as a function of codec and sample size

| | |
|--|---|
|  | <p>This appraisal must be treated with caution, as the utility of the G.729A codec is limited by various factors:</p> <ul style="list-style-type: none"> • The call is transferred uncompressed if one of the subscribers/circuits involved prevents compression • Connections with fax, modem and data terminal devices are only transferred uncompressed • External music and announcements are mostly transferred uncompressed (depends on the configuration (RCSU-CLASSMRK)) • Connections to a conference unit are mostly switched without compression (depends on the configuration (ZAND-IPDAVCCF)) <p>In all of these cases, either G.711 is used, or no codec at all.</p> <p>The bit rates for G.711 thus apply.</p> <p>In order to guarantee that bottlenecks are never encountered in the available bandwidth, the access point link must be designed for the G.711 bit rate.</p> |
|--|---|

By means of statistical appraisals, taking the actual configuration into account (how many fax/data devices are actually deployed, how many compression licenses are available, are all possible subscriber/access circuits configured for compression, how frequently are conferences used), a mixed calculation can be performed.

The load as a function of a sample size can only be used if it is ensured that all HiPath 4000 IPDA components are configured exclusively for this sample size. Otherwise, the worst value for the respective codec type would have to be used for reasons of reliability.

High-priority load of an access point as a function of the maximum number of B-channels

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 1 | 153 | 145 | 137 |
| 2 | 242 | 226 | 209 |
| 3 | 331 | 306 | 282 |
| 4 | 420 | 387 | 354 |
| 5 | 509 | 468 | 427 |
| 6 | 598 | 549 | 499 |
| 7 | 687 | 629 | 571 |
| 8 | 776 | 710 | 644 |
| 9 | 865 | 791 | 716 |
| 10 | 954 | 872 | 789 |
| 11 | 1,043 | 952 | 861 |
| 12 | 1,132 | 1,033 | 934 |
| 13 | 1,221 | 1,114 | 1,006 |
| 14 | 1,310 | 1,195 | 1,079 |
| 15 | 1,399 | 1,275 | 1,151 |
| 16 | 1,488 | 1,356 | 1,224 |
| 17 | 1,577 | 1,437 | 1,296 |
| 18 | 1,666 | 1,517 | 1,369 |
| 19 | 1,755 | 1,598 | 1,441 |
| 20 | 1,844 | 1,679 | 1,514 |
| 21 | 1,933 | 1,760 | 1,586 |
| 22 | 2,022 | 1,840 | 1,659 |
| 23 | 2,111 | 1,921 | 1,731 |
| 24 | 2,200 | 2,002 | 1,804 |
| 25 | 2,289 | 2,083 | 1,876 |

Table 6-8 High-priority load of an AP as a function of the permissible B-channels

Load Calculation

Load Calculation for Access Points

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 26 | 2,378 | 2,163 | 1,948 |
| 27 | 2,467 | 2,244 | 2,021 |
| 28 | 2,556 | 2,325 | 2,093 |
| 29 | 2,645 | 2,406 | 2,166 |
| 30 | 2,734 | 2,486 | 2,238 |
| 31 | 2,823 | 2,567 | 2,311 |
| 32 | 2,912 | 2,648 | 2,383 |
| 33 | 3,001 | 2,729 | 2,456 |
| 34 | 3,090 | 2,809 | 2,528 |
| 35 | 3,179 | 2,890 | 2,601 |
| 36 | 3,268 | 2,971 | 2,673 |
| 37 | 3,357 | 3,052 | 2,746 |
| 38 | 3,446 | 3,132 | 2,818 |
| 39 | 3,535 | 3,213 | 2,891 |
| 40 | 3,624 | 3,294 | 2,963 |
| 41 | 3,713 | 3,375 | 3,036 |
| 42 | 3,802 | 3,455 | 3,108 |
| 43 | 3,891 | 3,536 | 3,181 |
| 44 | 3,980 | 3,617 | 3,253 |
| 45 | 4,069 | 3,697 | 3,325 |
| 46 | 4,158 | 3,778 | 3,398 |
| 47 | 4,248 | 3,859 | 3,470 |
| 48 | 4,337 | 3,940 | 3,543 |
| 49 | 4,426 | 4,020 | 3,615 |
| 50 | 4,515 | 4,101 | 3,688 |
| 51 | 4,604 | 4,182 | 3,760 |
| 52 | 4,693 | 4,263 | 3,833 |
| 53 | 4,782 | 4,343 | 3,905 |

Table 6-8 High-priority load of an AP as a function of the permissible B-channels

Load Calculation
Load Calculation for Access Points

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 54 | 4,871 | 4,424 | 3,978 |
| 55 | 4,960 | 4,505 | 4,050 |
| 56 | 5,049 | 4,586 | 4,123 |
| 57 | 5,138 | 4,666 | 4,195 |
| 58 | 5,227 | 4,747 | 4,268 |
| 59 | 5,316 | 4,828 | 4,340 |
| 60 | 5,405 | 4,909 | 4,413 |
| 61 | 5,494 | 4,989 | 4,485 |
| 62 | 5,583 | 5,070 | 4,558 |
| 63 | 5,672 | 5,151 | 4,630 |
| 64 | 5,761 | 5,232 | 4,703 |
| 65 | 5,850 | 5,312 | 4,775 |
| 66 | 5,939 | 5,393 | 4,847 |
| 67 | 6,028 | 5,474 | 4,920 |
| 68 | 6,117 | 5,555 | 4,992 |
| 69 | 6,206 | 5,635 | 5,065 |
| 70 | 6,295 | 5,716 | 5,137 |
| 71 | 6,384 | 5,797 | 5,210 |
| 72 | 6,473 | 5,878 | 5,282 |
| 73 | 6,562 | 5,958 | 5,355 |
| 74 | 6,651 | 6,039 | 5,427 |
| 75 | 6,740 | 6,120 | 5,500 |
| 76 | 6,829 | 6,200 | 5,572 |
| 77 | 6,918 | 6,281 | 5,645 |
| 78 | 7,007 | 6,362 | 5,717 |
| 79 | 7,096 | 6,443 | 5,790 |
| 80 | 7,185 | 6,523 | 5,862 |
| 81 | 7,274 | 6,604 | 5,935 |

Table 6-8 High-priority load of an AP as a function of the permissible B-channels

Load Calculation

Load Calculation for Access Points

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 82 | 7,363 | 6,685 | 6,007 |
| 83 | 7,452 | 6,766 | 6,080 |
| 84 | 7,541 | 6,846 | 6,152 |
| 85 | 7,630 | 6,927 | 6,224 |
| 86 | 7,719 | 7,008 | 6,297 |
| 87 | 7,808 | 7,089 | 6,369 |
| 88 | 7,897 | 7,169 | 6,442 |
| 89 | 7,986 | 7,250 | 6,514 |
| 90 | 8,075 | 7,331 | 6,587 |
| 91 | 8,164 | 7,412 | 6,659 |
| 92 | 8,253 | 7,492 | 6,732 |
| 93 | 8,342 | 7,573 | 6,804 |
| 94 | 8,431 | 7,654 | 6,877 |
| 95 | 8,520 | 7,735 | 6,949 |
| 96 | 8,609 | 7,815 | 7,022 |
| 97 | 8,698 | 7,896 | 7,094 |
| 98 | 8,787 | 7,977 | 7,167 |
| 99 | 8,876 | 8,058 | 7,239 |
| 100 | 8,965 | 8,138 | 7,312 |
| 101 | 9,054 | 8,219 | 7,384 |
| 102 | 9,143 | 8,300 | 7,457 |
| 103 | 9,232 | 8,380 | 7,529 |
| 104 | 9,321 | 8,461 | 7,601 |
| 105 | 9,410 | 8,542 | 7,674 |
| 106 | 9,499 | 8,623 | 7,746 |
| 107 | 9,588 | 8,703 | 7,819 |
| 108 | 9,677 | 8,784 | 7,891 |
| 109 | 9,766 | 8,865 | 7,964 |

Table 6-8 High-priority load of an AP as a function of the permissible B-channels

Load Calculation
Load Calculation for Access Points

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 110 | 9,855 | 8,946 | 8,036 |
| 111 | 9,944 | 9,026 | 8,109 |
| 112 | 10,033 | 9,107 | 8,181 |
| 113 | 10,122 | 9,188 | 8,254 |
| 114 | 10,211 | 9,269 | 8,326 |
| 115 | 10,300 | 9,349 | 8,399 |
| 116 | 10,389 | 9,430 | 8,471 |
| 117 | 10,478 | 9,511 | 8,544 |
| 118 | 10,567 | 9,592 | 8,616 |
| 119 | 10,656 | 9,672 | 8,689 |
| 120 | 10,745 | 9,753 | 8,761 |

Table 6-8 High-priority load of an AP as a function of the permissible B-channels

Load Calculation

Load Calculation for a HG 3500

6.2 Load Calculation for a HG 3500

Calculation of the high-priority load for a HG 3500

| Protocol | Data type | Maximum bit rate/ port [Kbps] | Total bit rate [Kbps] with N payload ports | | |
|-------------------|-----------|-------------------------------------|---|--------------|---------------|
| | | | N=30 | N=60 | N=120 |
| RTP | VoIP | 88.8 | 2,664 | 5,328 | 10,656 |
| RTCP | VoIP | 0.2 | 6 | 12 | 25 |
| Total load | | | 2,670 | 5,340 | 10,681 |

Table 6-9 High-priority load of a HG 3500 (G.711/20 ms sample size)

In addition to high-priority load, low-priority load portions may also arise in certain situations for the following:

- SNMP queries via network management
- TAP/Service PC access at the access point
- FTP-loading of a new HG 3575 loadware as a background task

High-priority load of a HG 3500 as a function of codec type and sample size

| Codec type | Sample size | RTP load [Kbps] with N payload ports | | | Total Ethernet load [Kbps] with N payload ports | | |
|---------------|----------------|---|--------------|--------------|--|--------------|--------------|
| | | N=30 | N=60 | N=120 | N=30 | N=60 | N=120 |
| G.711 | 20 | 2,664 | 5,328 | 10,656 | 2,670 | 5,412 | 10,760 |
| G.711 | 30 | 2,416 | 4,832 | 9,664 | 2,490 | 4,916 | 9,768 |
| G.711 | 60 | 2,168 | 4,336 | 8,672 | 2,242 | 4,420 | 8,776 |
| G.729A | 20 | 984 | 1,968 | 3,936 | 1,058 | 2,052 | 4,040 |
| G.729A | 40 | 612 | 1,224 | 2,448 | 686 | 1,308 | 2,552 |
| G.729A | 60 | 488 | 976 | 1,952 | 562 | 1,060 | 2,056 |

Table 6-10 High-priority load of a HG 3500 as a function of codec and sample size



This appraisal must be treated with caution, as the utility of the G.729A codec is limited by various factors:

- The call is transferred uncompressed if one of the subscribers/circuits involved prevents compression
- Connections with fax, modem and data terminal devices are only transferred uncompressed
- External music and announcements are mostly transferred uncompressed (depends on the configuration (RCSU-CLASSMRK))
- Connections to a conference unit are mostly switched without compression (depends on the configuration (ZAND-IPDAVCCF))

In all of these cases, either G.711 is used, or no codec at all.

The bit rates for G.711 thus apply.

In order to guarantee that bandwidth bottlenecks are never encountered, the access point link must be designed for the G.711 bit rate.

By means of statistical appraisals, taking the actual configuration into account (how many fax/data devices are actually deployed, how many compression licenses are available, are all possible subscriber/access circuits configured for compression, how frequently are conferences used), a mixed calculation can be performed.

The load as a function of a sample size can only be used if it is ensured that all HiPath 4000 IPDA components are configured exclusively for this sample size. Otherwise, the worst value for the respective codec type would have to be used for reasons of reliability.

High-priority load of a HG 3500 as a function of the maximum number of B-channels

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 1 | 89 | 81 | 72 |
| 2 | 178 | 161 | 145 |
| 3 | 267 | 242 | 217 |
| 4 | 356 | 323 | 290 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

Load Calculation

Load Calculation for a HG 3500

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 5 | 445 | 404 | 362 |
| 6 | 534 | 484 | 435 |
| 7 | 623 | 565 | 507 |
| 8 | 712 | 646 | 580 |
| 9 | 801 | 727 | 652 |
| 10 | 890 | 807 | 725 |
| 11 | 979 | 888 | 797 |
| 12 | 1,068 | 969 | 870 |
| 13 | 1,157 | 1,050 | 942 |
| 14 | 1,246 | 1,130 | 1,015 |
| 15 | 1,335 | 1,211 | 1,087 |
| 16 | 1,424 | 1,292 | 1,160 |
| 17 | 1,513 | 1,373 | 1,232 |
| 18 | 1,602 | 1,453 | 1,305 |
| 19 | 1,691 | 1,534 | 1,377 |
| 20 | 1,780 | 1,615 | 1,449 |
| 21 | 1,869 | 1,696 | 1,522 |
| 22 | 1,958 | 1,776 | 1,594 |
| 23 | 2,047 | 1,857 | 1,667 |
| 24 | 2,136 | 1,938 | 1,739 |
| 25 | 2,225 | 2,019 | 1,812 |
| 26 | 2,314 | 2,099 | 1,884 |
| 27 | 2,403 | 2,180 | 1,957 |
| 28 | 2,492 | 2,261 | 2,029 |
| 29 | 2,581 | 2,341 | 2,102 |
| 30 | 2,670 | 2,422 | 2,174 |
| 31 | 2,759 | 2,503 | 2,247 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

Load Calculation
Load Calculation for a HG 3500

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 32 | 2,848 | 2,584 | 2,319 |
| 33 | 2,937 | 2,664 | 2,392 |
| 34 | 3,026 | 2,745 | 2,464 |
| 35 | 3,115 | 2,826 | 2,537 |
| 36 | 3,204 | 2,907 | 2,609 |
| 37 | 3,293 | 2,987 | 2,682 |
| 38 | 3,382 | 3,068 | 2,754 |
| 39 | 3,471 | 3,149 | 2,827 |
| 40 | 3,560 | 3,230 | 2,899 |
| 41 | 3,649 | 3,310 | 2,971 |
| 42 | 3,738 | 3,391 | 3,044 |
| 43 | 3,827 | 3,472 | 3,116 |
| 44 | 3,916 | 3,553 | 3,189 |
| 45 | 4,005 | 3,633 | 3,261 |
| 46 | 4,094 | 3,714 | 3,334 |
| 47 | 4,183 | 3,795 | 3,406 |
| 48 | 4,272 | 3,876 | 3,479 |
| 49 | 4,361 | 3,956 | 3,551 |
| 50 | 4,450 | 4,037 | 3,624 |
| 51 | 4,539 | 4,118 | 3,696 |
| 52 | 4,628 | 4,199 | 3,769 |
| 53 | 4,717 | 4,279 | 3,841 |
| 54 | 4,806 | 4,360 | 3,914 |
| 55 | 4,895 | 4,441 | 3,986 |
| 56 | 4,984 | 4,522 | 4,059 |
| 57 | 5,073 | 4,602 | 4,131 |
| 58 | 5,162 | 4,683 | 4,204 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

Load Calculation

Load Calculation for a HG 3500

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 59 | 5,251 | 4,764 | 4,276 |
| 60 | 5,340 | 4,844 | 4,348 |
| 61 | 5,429 | 4,925 | 4,421 |
| 62 | 5,518 | 5,006 | 4,493 |
| 63 | 5,608 | 5,087 | 4,566 |
| 64 | 5,697 | 5,167 | 4,638 |
| 65 | 5,786 | 5,248 | 4,711 |
| 66 | 5,875 | 5,329 | 4,783 |
| 67 | 5,964 | 5,410 | 4,856 |
| 68 | 6,053 | 5,490 | 4,928 |
| 69 | 6,142 | 5,571 | 5,001 |
| 70 | 6,231 | 5,652 | 5,073 |
| 71 | 6,320 | 5,733 | 5,146 |
| 72 | 6,409 | 5,813 | 5,218 |
| 73 | 6,498 | 5,894 | 5,291 |
| 74 | 6,587 | 5,975 | 5,363 |
| 75 | 6,676 | 6,056 | 5,436 |
| 76 | 6,765 | 6,136 | 5,508 |
| 77 | 6,854 | 6,217 | 5,581 |
| 78 | 6,943 | 6,298 | 5,653 |
| 79 | 7,032 | 6,379 | 5,725 |
| 80 | 7,121 | 6,459 | 5,798 |
| 81 | 7,210 | 6,540 | 5,870 |
| 82 | 7,299 | 6,621 | 5,943 |
| 83 | 7,388 | 6,702 | 6,015 |
| 84 | 7,477 | 6,782 | 6,088 |
| 85 | 7,566 | 6,863 | 6,160 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

Load Calculation
Load Calculation for a HG 3500

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 86 | 7,655 | 6,944 | 6,233 |
| 87 | 7,744 | 7,024 | 6,305 |
| 88 | 7,833 | 7,105 | 6,378 |
| 89 | 7,922 | 7,186 | 6,450 |
| 90 | 8,011 | 7,267 | 6,523 |
| 91 | 8,100 | 7,347 | 6,595 |
| 92 | 8,189 | 7,428 | 6,668 |
| 93 | 8,278 | 7,509 | 6,740 |
| 94 | 8,367 | 7,590 | 6,813 |
| 95 | 8,456 | 7,670 | 6,885 |
| 96 | 8,545 | 7,751 | 6,958 |
| 97 | 8,634 | 7,832 | 7,030 |
| 98 | 8,723 | 7,913 | 7,103 |
| 99 | 8,812 | 7,993 | 7,175 |
| 100 | 8,901 | 8,074 | 7,247 |
| 101 | 8,990 | 8,155 | 7,320 |
| 102 | 9,079 | 8,236 | 7,392 |
| 103 | 9,168 | 8,316 | 7,465 |
| 104 | 9,257 | 8,397 | 7,537 |
| 105 | 9,346 | 8,478 | 7,610 |
| 106 | 9,435 | 8,559 | 7,682 |
| 107 | 9,524 | 8,639 | 7,755 |
| 108 | 9,613 | 8,720 | 7,827 |
| 109 | 9,702 | 8,801 | 7,900 |
| 110 | 9,791 | 8,882 | 7,972 |
| 111 | 9,880 | 8,962 | 8,045 |
| 112 | 9,969 | 9,043 | 8,117 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

Load Calculation

Load Calculation for a HG 3500

| Maximum permissible number of B-channels | Total Ethernet load at G.711/20ms [Kbps] | Total Ethernet load at G.711/30ms [Kbps] | Total Ethernet load at G.711/60ms [Kbps] |
|--|--|--|--|
| 113 | 10,058 | 9,124 | 8,190 |
| 114 | 10,147 | 9,205 | 8,262 |
| 115 | 10,236 | 9,285 | 8,335 |
| 116 | 10,325 | 9,366 | 8,407 |
| 117 | 10,414 | 9,447 | 8,480 |
| 118 | 10,503 | 9,527 | 8,552 |
| 119 | 10,592 | 9,608 | 8,624 |
| 120 | 10,681 | 9,689 | 8,697 |

Table 6-11 High-priority load of a HG 3500 as a function of the permissible number of B-channels

6.3 Calculation Basis - Configuring Payload Packets

6.3.1 Configuring Ethernet MAC Frames

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------------------|---------------------------------------|---|---|---|---|---|---|---|
| Preamble (1) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (2) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (3) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (4) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (5) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (6) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (7) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Preamble (8) | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| Destination Address | MAC Destination Address (6 Bytes) | | | | | | | |
| Destination Address | | | | | | | | |
| Destination Address | | | | | | | | |
| Destination Address | | | | | | | | |
| Destination Address | | | | | | | | |
| Destination Address | | | | | | | | |
| Source Address | MAC Source Address (6 Bytes) | | | | | | | |
| Source Address | | | | | | | | |
| Source Address | | | | | | | | |
| Source Address | | | | | | | | |
| Source Address | | | | | | | | |
| Source Address | | | | | | | | |
| 802.1Q Tag Type | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 802.1Q Tag Type | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 802.1Q Tag Control | P | P | P | 0 | 0 | 0 | 0 | 0 |
| 802.1Q Tag Control | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Type | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Type | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IP Frame | MAC Payload | | | | | | | |
| Frame Check Sequence | FCS | | | | | | | |
| Frame Check Sequence | | | | | | | | |
| Frame Check Sequence | | | | | | | | |
| Frame Check Sequence | | | | | | | | |

Table 6-12 Configuring Ethernet MAC frames for IPDA payload

Load Calculation

Calculation Basis - Configuring Payload Packets

6.3.2 Configuring IP Frames

IPDA RTP Packets

| | | 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 | | | | | | | |
|---|----------------|---|--|---|---|--------------|-----------------|----|--|
| IP Header | Version | IHL | Type Of Service | Total Length | | | | | |
| | Identification | | Flags | Fragment Offset | | | | | |
| | Time to Live | | Protocol | Header Checksum | | | | | |
| | Source Address | | Destination Address | | | | | | |
| | Source Port | | Destination Port | | | | | | |
| UDP Header | Length | | Checksum | | | | | | |
| | V | P | X | CC | M | Payload Type | Sequence Number | | |
| RTP Header | Timestamp | | Synchronization Source (SSRC) Identifier | | | | | | |
| | Data | | | | | | | | |
| Version | | Version of Internet Header | | 4 | | | | | |
| IHL | | Internet Header Length | | 20 | | | | | |
| Type Of Service | | Type of Service / Packet Handling Behavior Class acc. To DiffServ - Administrated Value | | | | | | | |
| Total Length | | Length of IP datagram including header | | 160/280/400/520 for G.711 with 15/30/45/60 msec Audio | | | | | |
| | | | | 60/80/100 for G.729 with 20/40/60 msec Audio | | | | | |
| Identification | | ID to assemble fragments of datagram | | | | | | | |
| Flags | | set to May fragment, Last fragment | | 0 | | | | | |
| Fragment Offset | | sent unfragmented -> no offset | | 0 | | | | | |
| Time to Live | | decremented by each instance the datagram passes | | | | | | 17 | |
| Protocol | | UDP | | | | | | | |
| Header Checksum | | Checksum on IP Header only | | | | | | | |
| Source Address | | IP Address | | | | | | | |
| Destination Address | | IP Address | | | | | | | |
| Source Port | | | | | | | | | |
| Destination Port | | | | | | | | | |
| Length | | Length of UDP datagram including UDP header | | 140/260/380/500 for G.711 with 15/30/45/60 msec Audio | | | | | |
| | | | | 40/60/80 for G.729 with 20/40/60 msec Audio | | | | | |
| Checksum | | Checksum over IP Header, UDP Header und UDP Data | | | | | | | |
| V | | Version of RTP | | 2 | | | | | |
| P | | Padding | | 0 | | | | | |
| X | | Extension | | 0 | | | | | |
| CC | | Contributing Source (CSRC) identifiers | | 0 | | | | | |
| M | | Marker | | 0 | | | | | |
| Payload Type | | Payload Type (G.711 µ-law = PCMU = 0 / G.711 A-law = PCMA = 8 / G.729A = ???) | | 0/8/18 | | | | | |
| Sequence Number | | Incremented by 1 with each RTP packet - initial value is random | | | | | | | |
| Timestamp | | Timestamp for 1st sample in packet - incremented by 1 for each sampling period - every 125 µsec | | | | | | | |
| Synchronization Source (SSRC) Identifier | | chosen randomly, valid only per session | | | | | | | |

Table 6-13 Configuring IP frames for IPDA payload

7 Local Access Point Administration at CLI via Terminal

If an LCT/service PC running “HiPath 4000 Expert Access“ is not available for the local configuration of an access point, the administration may also be performed directly via a terminal or terminal emulation, if necessary.

The RS 232 / V.24 interface at the 3575 is labeled with “Service“ and is set to 38400 Baud, 8 Bit, no Parity.

The Command Line Interface issues the following message after you press



Please log in.

Username:

Login data

1. new board (before installation)

Login: HP4K-DEVEL

Password: Siemens2000

2. after installation (HiPath steuert NCUI4)

Login: TRM

Password: HICOM

If the module was already in operation and if the WBM login and password were changed, then the values set apply.

The following is displayed after successful login:

```
Welcome to the HG 3575 v4.0 <LW-version> Command Line
Interpreter.

vxTarget>
```

After the prompt, the necessary parameters can now be entered.

A list of available commands can be now requested via the local help function which is available via the `help` command.

The CLI does not distinguish between “direct link“ and “networked“ access points. The designation of the parameters reflects the programming name of the loadware. As already mentioned, direct operation of the CLI without the “HiPath 4000 Expert Access“ application is only an emergency solution.

The following tables are intended to assist in finding the correct content for the parameters. The tables list the requisite CLI parameters and arrange them in relationship to the AMO parameters from which the values have to be derived:

7.1 Networked access point

NOTE: In order to be able to carry out the following commands, you will need ADMIN rights in CLI.

| CLI parameter name | Parameter meaning | AMO - Branch - Parameter |
|--------------------|--|--|
| ip_addr_eth | IP address of the access point | APRT TYPE=APNET - APIPADDR |
| netmask_eth | Netmask in the network of the access point | APRT TYPE=APNET - NETMASK |
| default_gateway | IP address of the default router in the network of the access point | UCSU UNIT=AP - APRTADDR |
| ip_addr_signalling | IP address of the access point | APRT TYPE=APNET - APIPADDR |
| netmask_signalling | Netmask in the network of the access point | APRT TYPE=APNET - NETMASK |
| ip_addr_CC_A | IP address of the CC-A | SIPCO TYPE=LSNET - CCAADDR |
| ip_addr_CC_B | IP address of the CC-B | SIPCO TYPE=LSNET - CCBADDR |
| netmask_hhs | HiPath 4000 LAN segment netmask | SIPCO TYPE=LSNET - NETMASK |
| ip_addr_tap | IP address for TAP link | APRT TYPE=APNET - TAIPADDR |
| vlan_tag | VLAN tagging on/off [0 = OFF, 1 = ON] | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN |
| vlan_id | VLAN ID [0.. 4095] | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID |
| eth_link_mode | Ethernet interface operating mode 0 : Autonegotiation 21 : 10 Mbps half duplex 22 : 10 Mbps full duplex 23 : 100 Mbps half duplex 24 : 100 Mbps full duplex | STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 Mbps, half duplex 10MBFD: 10 Mbps, full duplex 100MBHD: 100 Mbps, half duplex 100MBFD: 100 Mbps, full duplex |

Table 23

CLI parameter for “networked” access point

Note

For “networked” access points

- **ip_addr_signalling = ip_addr_eth**
and
- **netmask_signalling = netmask_eth**

must be set!

The command syntax is

```
set ip address Parameter name Value or
set id Parameter name Value
```

For Access Point 99 from the configuration examples (see Figure 20 HiPath 4000 LAN segment on page 4-38 and Figure 22 Configuring a “Networked” access point on page 4-58), the following command syntax is yielded:

```
get write access
set ip address ip_addr_eth 192.168.23.99
set ip address netmask_eth 255.255.255.0
set ip address default_gateway 192.168.23.1
set ip address ip_addr_signalling 192.168.23.99
set ip address netmask_signalling 255.255.255.0
set ip address ip_addr_CC_A 192.168.1.1
set ip address ip_addr_CC_B 192.168.1.1
set ip address netmask_hhs 255.255.255.0
set ip address ip_addr_tap 192.168.23.199
set id vlan_tag 0
set id vlan_id 0
set id eth_link_mode 0
finish
```

NOTE: No other commands (e.g. show) may be transmitted between the set commands and the finish command, which transfers the data to the Flash memory.

7.2 Direct link access point

NOTE: In order to be able to execute the following commands, you will need ADMIN rights in CLI.

| CLI parameter name | Parameter | AMO - Branch - Parameter |
|--------------------|---|-------------------------------|
| ip_addr_eth | IP address of the access point in the HiPath 4000 LAN segment | UCSU UNIT=AP - LSRTADDR |
| netmask_eth | HiPath 4000 LAN segment network mask | SIPCO TYPE=LSNET - NETMASK |
| default_gateway | IP address of the default router in the HiPath 4000 LAN segment | UCSU UNIT=AP - APRTADDR |
| ip_addr_signalling | IP address of the access point in the internal AP network segment | APRT TYPE=APNET - APIPADDR |

Table 24

CLI parameters for “direct link” access point

Local Access Point Administration at CLI via Terminal

Direct link access point

| CLI parameter name | Parameter | AMO - Branch - Parameter |
|--------------------|--|--|
| netmask_signalling | Netmask of the internal AP network segment | APRT TYPE=APNET - NETMASK |
| ip_addr_CC_A | IP address of the CC-A | SIPCO TYPE=LSNET - CCAADDR |
| ip_addr_CC_B | IP address of the CC-B | SIPCO TYPE=LSNET - CCBADDR |
| netmask_hhs | HiPath 4000 LAN segment network mask | SIPCO TYPE=LSNET - NETMASK |
| ip_addr_tap | IP address for TAP link | APRT TYPE=APNET - TAIPADDR |
| vlan_tag | VLAN tagging on/off [0 = OFF,1 = ON] | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLAN |
| vlan_id | VLAN ID [0.. 4095] | STMIB: MTYPE=NCUI2, TYPE=IFDATA - VLANID |
| eth_link_mode | Ethernet interface operating mode 0 : Autonegotiation 21 : 10 Mbps half duplex 22 : 10 Mbps full duplex 23 : 100 Mbps half duplex 24 : 100 Mbps full duplex | STMIB: MTYPE=NCUI2, TYPE=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 Mbps, half duplex 10MBFD: 10 Mbps, full duplex 100MBHD: 100 Mbps, half duplex 100MBFD: 100 Mbps, full duplex |

Table 24

CLI parameters for “direct link” access point

The command syntax is

```
set ip address Parameter name Value or
set id Parameter name Value
```

For Access Point 17 from the configuration examples (see Figure 20 HiPath 4000 LAN segment on page 4-38 and Figure 23 Configuring a “Direct Link” access point on page 4-68), the following command syntax is yielded:

```
get write access
set ip address ip_addr_eth 192.168.1.17
set ip address netmask_eth 255.255.255.0
set ip address default_gateway 192.168.1.254
set ip address ip_addr_signalling 192.168.200.1
set ip address netmask_signalling 255.255.255.252
set ip address ip_addr_CC_A 192.168.1.1
set ip address ip_addr_CC_B 192.168.1.2
set ip address netmask_hhs 255.255.255.0
set ip address ip_addr_tap 192.168.200.2
set id vlan_tag 0
set id vlan_id 0
set id eth_link_mode 0
finish
```

NOTE: No other commands (e.g. `show`) may be transmitted between the `set` commands and the `finish` command, which transfers the data to the Flash memory.

7.3 Additional settings for the initial startup

To facilitate immediate diagnostic access to the access point in the initial configuration, the corresponding parameters can be changed in the CLI.

NOTE: In order to be able to execute the following commands, you will need ADMIN rights in CLI.

| CLI parameter name | Parameter | AMO - Branch - Parameter |
|--------------------|---|---|
| debug_details | Debug Details Controls which messages/events are stored. The entire value to be set is the total of the entries of the individual switch: 1 : record HHS messages (from HiPath 4000) 2 : record error messages 4 : record switch messages 8 : record trace messages 16 : record events Total must be at least two, i.e. error messages must always be set | STMIB : MTYPE=NCUI2, TYPE=DEBUG - DEBUGDET HHSMS : record HHS messages (from HiPath 4000) ERRORMS : record error messages SWITCHMS : record switch messages TRACES : record trace messages EVENT : record events |
| file_access_mode | Facility access mode Controls access via LAN to HTTP, TELNET, FTP and SNMP 0: Access denied, SNMP possible 1: Access possible, SNMP possible 2: Access denied, SNMP denied | STMIB: MTYPE=NCUI2, TYPE=DEBUG - FACCMODE |

Table 25 Additional CLI parameters for diagnostic access

These values are configured by the following command lines:

```

get write access
set id debug_details 0
set id file_access_mode 0
finish
  
```

NOTE: No other commands (e.g. show) may be transmitted between the `set` commands and the `finish` command, which transfers the data to the Flash memory.

The parameters configured on the HG 3575 can be called up via the CLI through the command `show all parameters`.

7.4 Assignment of parameter names in LW-CLI to the AMO parameters

Finally, the following table provides an overview of all CLI parameters and their assignment to AMO parameters.

| Parameter name in LW-CLI | | Parameter name | AMO | Branch |
|--------------------------|----|---|---------------|----------------------------|
| ip_addr_eth | * | APDL: LSRTADDR APNW: APIPADDR | UCSU APRT | UNIT=AP TYPE=APNET |
| netmask_eth | * | APDL: NETMASK APNW: NETMASK | SIPCO APRT | TYPE=LSNET TYPE=APNET |
| default_gateway | *1 | APRTADDR | UCSU | UNIT=AP |
| ip_addr_signalling | * | APIPADR | APRT | TYPE=APNET |
| netmask_signalling | * | NETMASK | APRT | TYPE=APNET |
| ip_addr_survivability | *2 | SURVNET (last byte identical to LTU - UCSU) | SIPCO | TYPE=LSNET |
| netmask_survivability | *2 | fix: 255.255.255.0 | - | - |
| gateway_survivability | *2 | SURVNET (last byte identical to ROUTERNO - TYPE=SURV -APRT) | SIPCO | TYPE=LSNET |
| netmask_hhs | * | NETMASK | SIPCO | TYPE=LSNET |
| ip_addr_CC_A | * | CCAADDR | SIPCO | TYPE=LSNET |
| ip_addr_CC_B | *3 | CCBADDR | SIPCO | TYPE=LSNET |
| ip_addr_tap | | TAIPADDR | APRT | TYPE=APNET |
| vlan_tag | | VLAN | STMIB | MTYPE=NCUI2 TYPE=IFDATA |
| vlan_id | | VLANID | STMIB | MTYPE=NCUI2 TYPE=IFDATA |
| eth_link_mode | | BITRATE | STMIB | MTYPE=NCUI2 TYPE=IFDATA |
| debug_details | | DEBUGDET | STMIB | MTYPE=NCUI2 TYPE=DEBUG |
| file_access_mode | | FACCMODE | STMIB | MTYPE=NCUI2 TYPE=DEBUG |
| server_port_signaling | | fix: 4000 | - | - |
| keep_alive_time_signal | | ALVTIME | SIPCO | TYPE=TIMING |
| reset_timer_sign_loss | | RESTIME | SIPCO | TYPE=TIMING |
| server_port_supervisory | | fix: 4001 | - | - |
| tos_lan | | TOSLAN | STMIB | MTYPE=NCUI2 TYPE=IFDATA |

Table 26

Assignment of parameter names in LW-CLI to the AMO parameters

Local Access Point Administration at CLI via Terminal
Assignment of parameter names in LW-CLI to the AMO parameters

| Parameter name in LW-CLI | | Parameter name | AMO | Branch |
|-----------------------------|----|--|-------|----------------------------|
| tos_modem | | TOSMODEM | STMIB | MTYPE=NCUI2 TYPE=IFDATA |
| survability_enable | *2 | derived from ip_addr_survability > 0.0.0.0 | - | - |

Table 26 Assignment of parameter names in LW-CLI to the AMO parameters

- * Requisite parameters for first-time initialization of NCUI2/4
- *1 Requisite parameters for first-time initialization of NCUI2/4 for “networked” access points
- *2 Requisite parameters for first-time initialization of NCUI2/4 with *signaling survivability*
- *3 Requisite parameters for first-time initialization of NCUI2/4 at *duplex systems*

In the case of some parameters, a distinction must be made according to the type of connection configured CONNTYPE - UNIT=AP - UCSU. In this case, different assignments are required for APDL and APNW.

<LW-version>

<LW-version> holds the currently loaded loadware version number (e.g. L0-TOS.10.030-004)

Local Access Point Administration at CLI via Terminal

Assignment of parameter names in LW-CLI to the AMO parameters

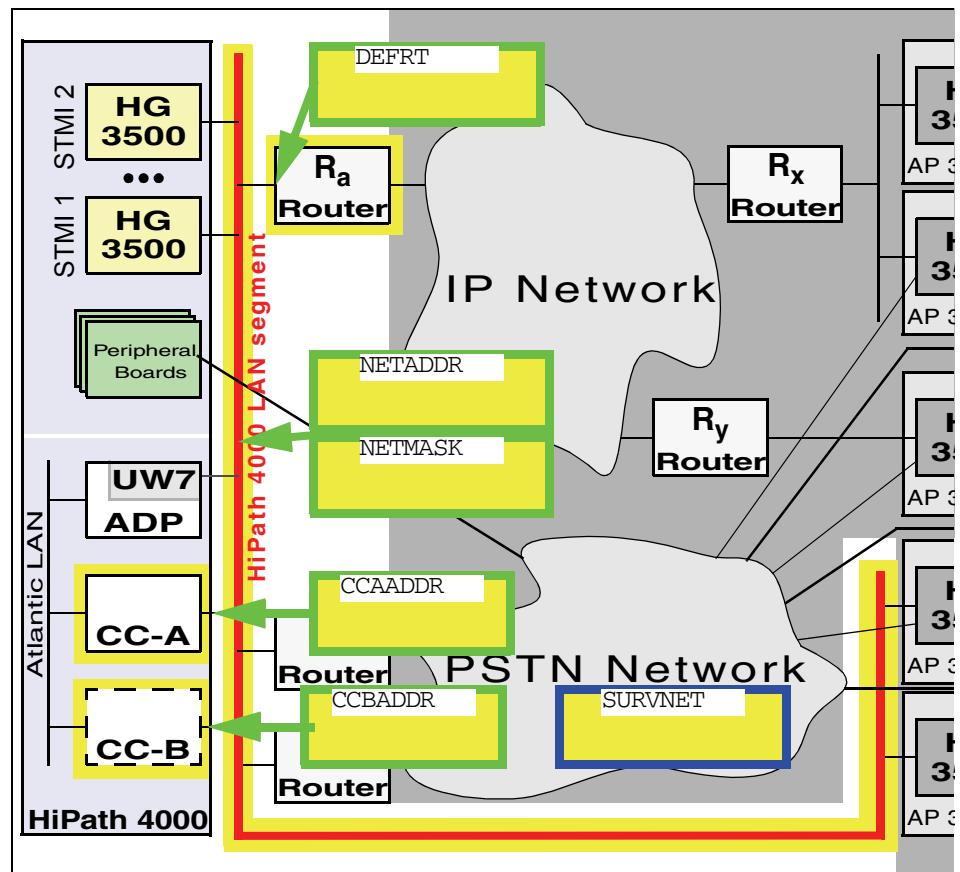
8 Spreadsheets - IPDA Configuration

The following spreadsheets are designed to help you perform an IPDA configuration. Each of the sheets has a configuration diagram and a blank AMO template on one side, and the completed example from the Service Manual on the other.

The following spreadsheets (with example) are available:

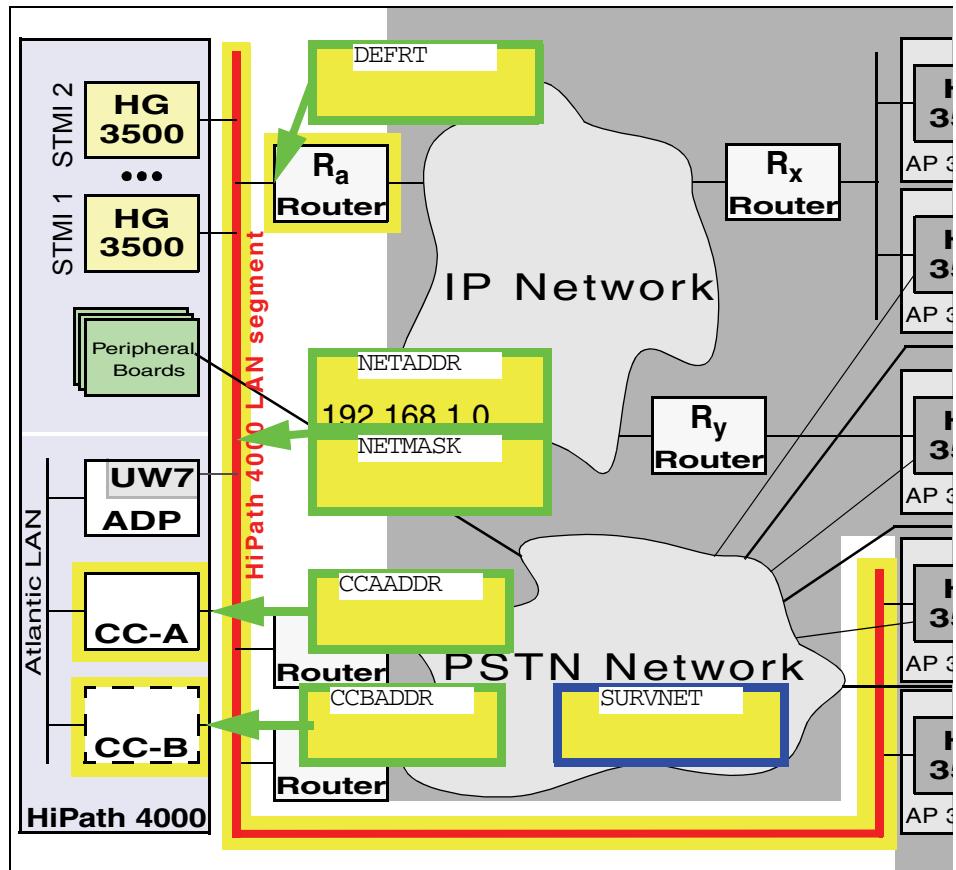
- Spreadsheet: Configuring the HiPath 4000 LAN segment
- Spreadsheet: Configuring a “networked” access point
- Spreadsheet: Configuring a “direct link” access point
- Spreadsheet: Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 system
- AP Emergency spreadsheet: configuring a CC-AP
- AP Emergency spreadsheet: emergency group

Spreadsheet: Configuring the HiPath 4000 LAN segment



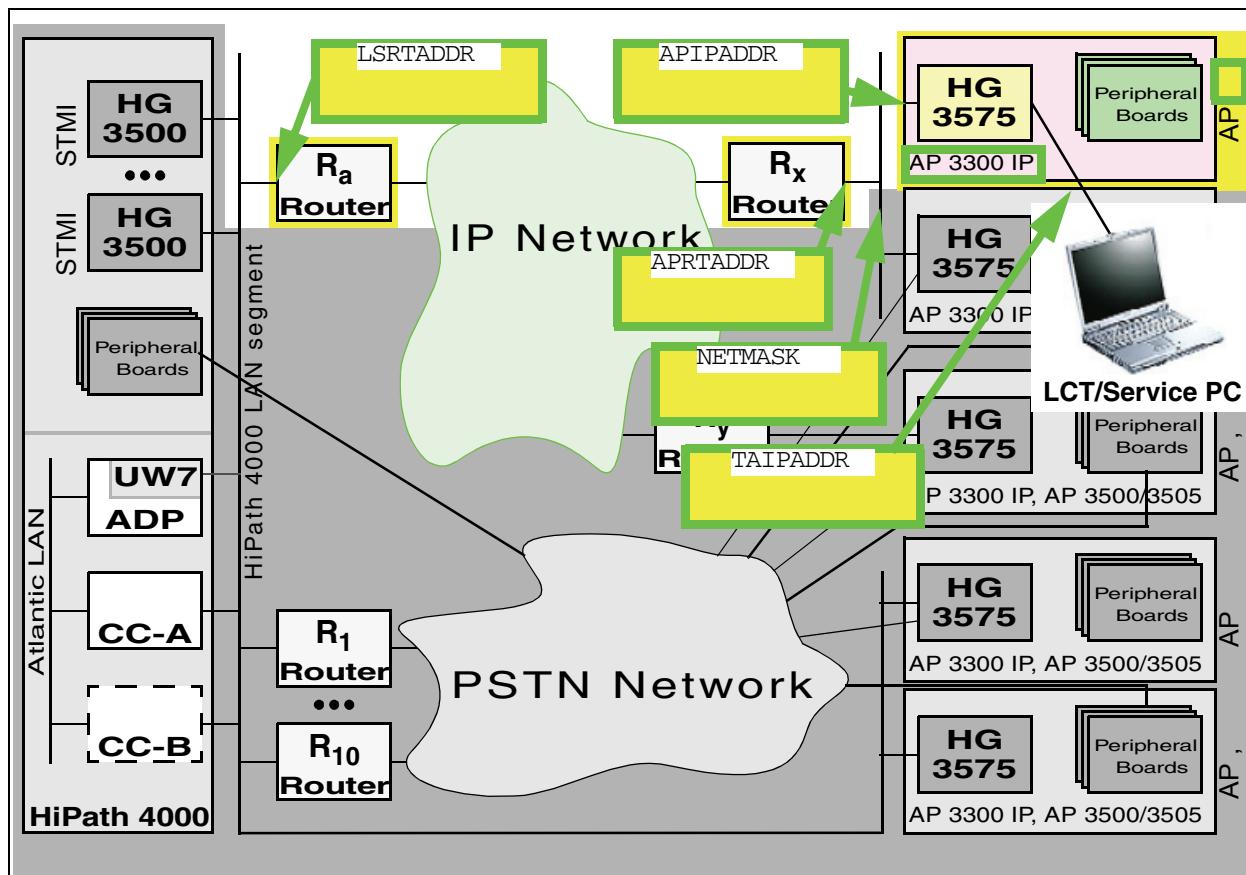
| | | |
|--------------------|---------------------|--------------------|
| ADD-SIPCO: | NETADDR= , | NETMASK= , |
| | , | , |
| DEFRT= , | CCAADDR= , | |
| CCBADDR= , | SURVNET= 0; | |
| | , | |

Sample Sheet: Configuring the HiPath 4000 LAN segment



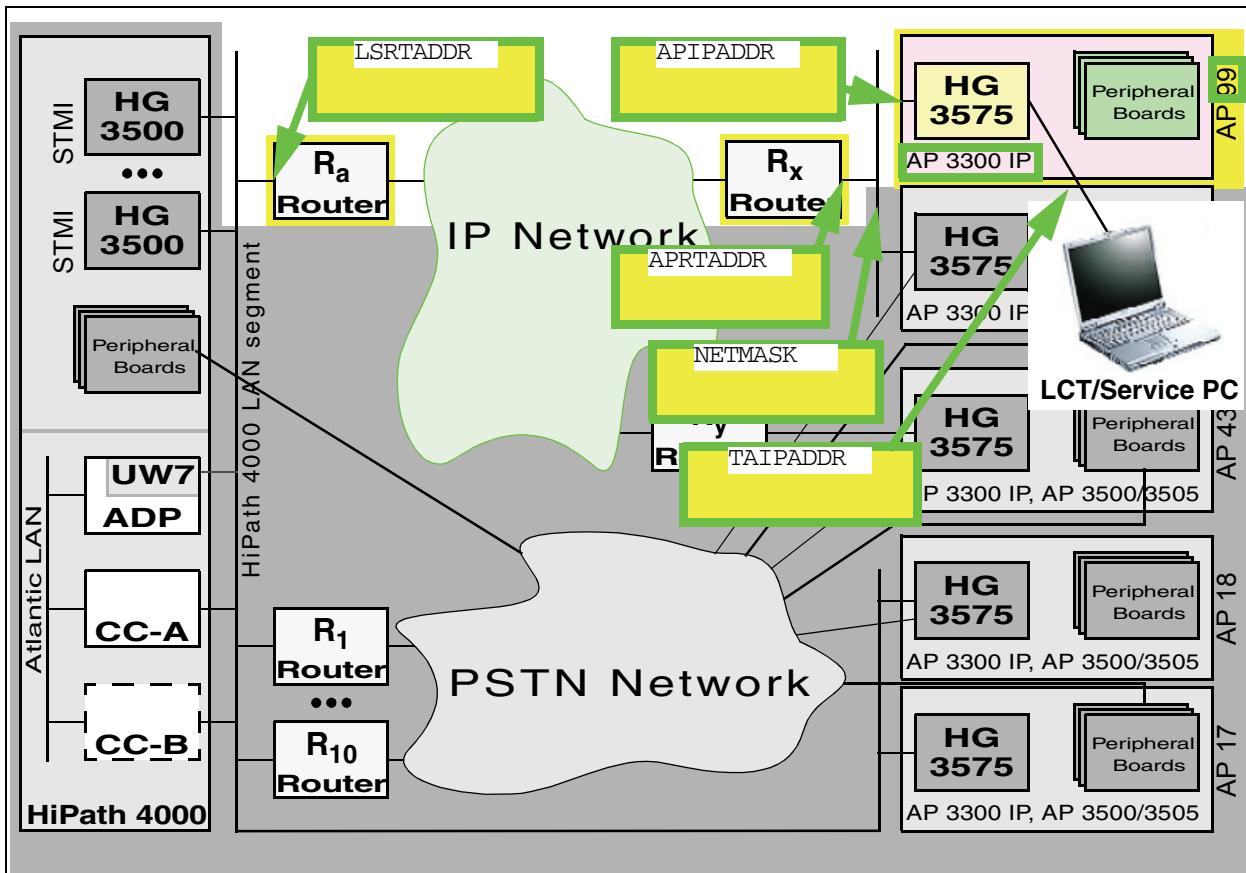
| | | |
|------------|----------------------|------------------------|
| ADD-SIPCO: | NETADDR=192.168.1.0, | NETMASK=255.255.255.0, |
| | DEFRT=192.168.1.254, | CCAADDR=192.168.1.1, |
| | CCBADDR=192.168.1.2, | SURVNET=192.168.15.0; |

Spreadsheet: Configuring a “networked” access point



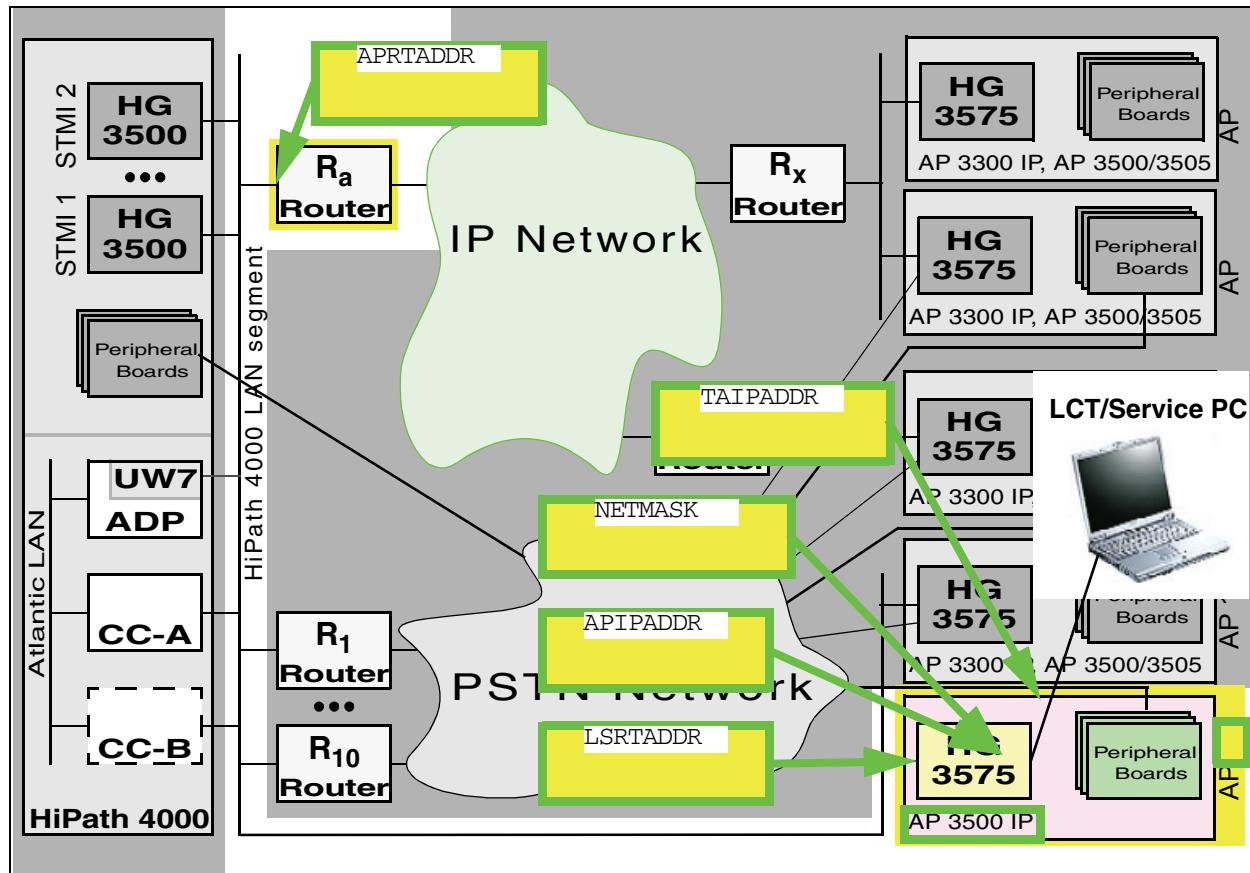
| | | |
|-----------|-------------------|-------------------|
| ADD-UCSU: | UNIT=AP, | LTU= , |
| | LTPARTNO=Q23 -X , | SRCGRP= , |
| | FRMTYPE= , | CONNTYPE=APNW , |
| | LSRTADDR= . . . , | APRTADDR= . . . , |
| | LOCID= , | LOCATION= " |
| | | " , |
| | PHONE= , | FAX= , |
| | PLCHECK= , | BCHLCNT= , |
| | CONVLAW= ; | |
| ADD-APRT: | TYPE=APNET , | LTU= , |
| | APIPADDR= . . . , | NETMASK= . . . , |
| | TAIPADDR= . . . ; | |

Sample Sheet: Configuring a “networked” access point



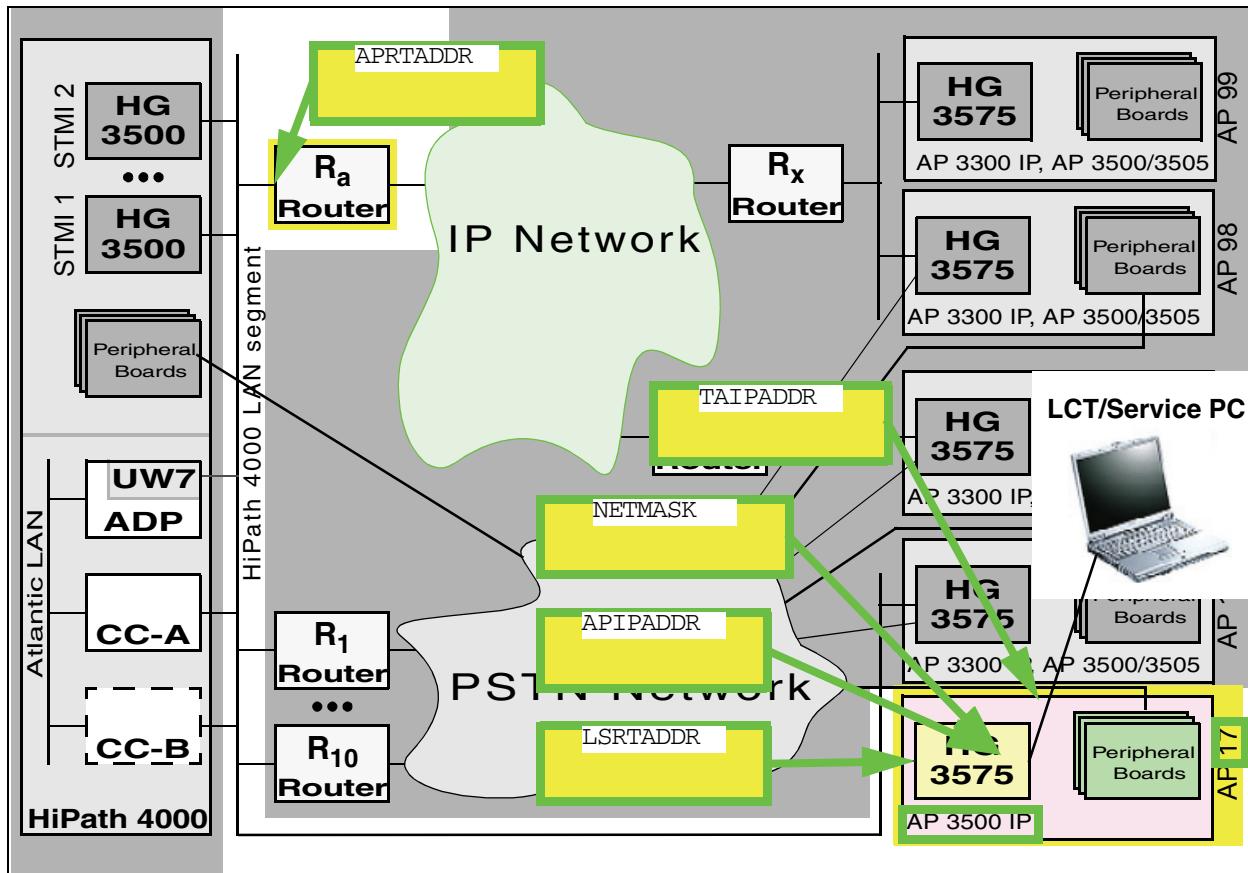
| | | |
|-----------|--------------------------|------------------------|
| ADD-UCSU: | UNIT=AP, | LTU=99, |
| | LTPARTNO=Q2305-X35, | SRCGRP=2, |
| | FRMTYPE=AP 9837009, | CONNTYPE=APNW, |
| | LSRTADDR=192.168.1.254, | APRTADDR=192.168.23.1, |
| | LOCID=2, | LOCATION="BLN ROHRDAMM |
| | | 85. GEB. 30-222", |
| | PHONE=03038612345, | FAX=03038654321, |
| | PLCHECK=YES, | BCHLCNT=40, |
| | CONVLAW=NO; | |
| ADD-APRT: | TYPE=APNET, | LTU=99, |
| | APIPADDR=192.168.23.99, | NETMASK=255.255.255.0, |
| | TAIPADDR=192.168.23.199; | |

Spreadsheet: Configuring a “direct link” access point



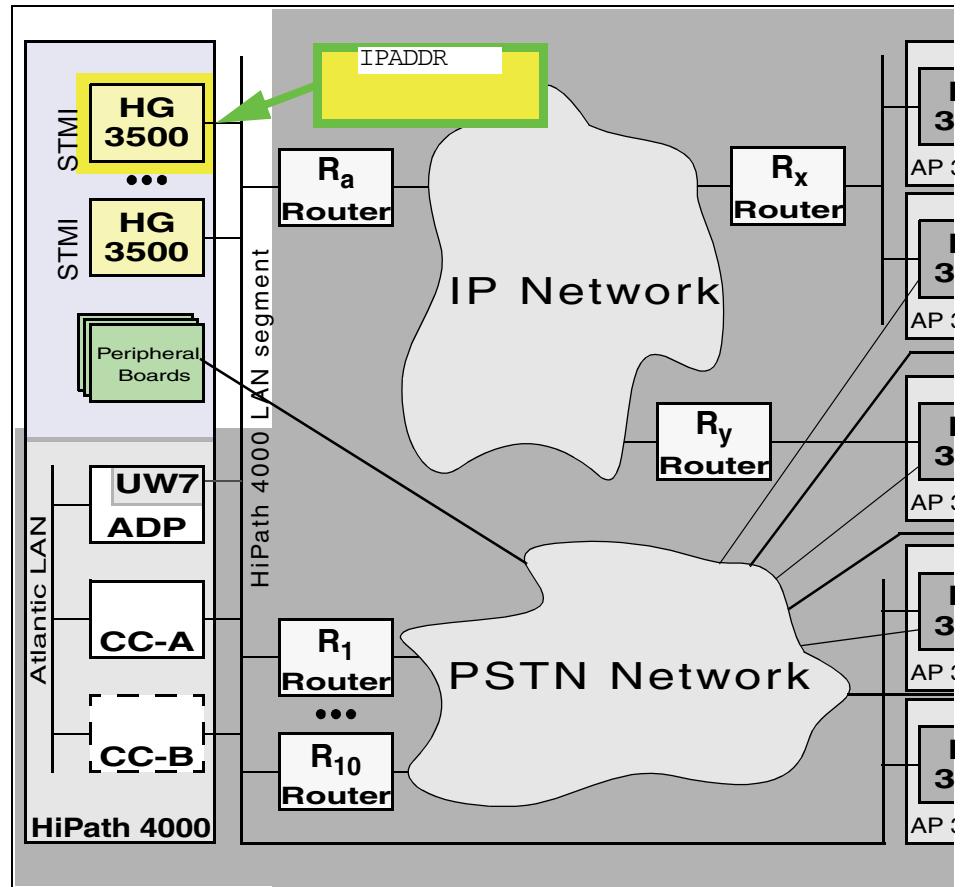
| | | |
|-----------|-------------------|-------------------|
| ADD-UCSU: | UNIT=AP, | LTU= , |
| | LTPARTNO=Q23 -X , | SRCGRP= , |
| | FRMTYPE= , | CONNTYPE=APDL , |
| | LSRTADDR= . . . , | APRTADDR= . . . , |
| | LOCID= , | LOCATION=" " |
| | | " , |
| | PHONE= , | FAX= , |
| | PLCHECK= , | BCHLCNT= , |
| | CONVLAW= ; | |
| ADD-APRT: | TYPE=APNET, | LTU= , |
| | APIPADDR= . . . , | NETMASK= . . . , |
| | TAIPADDR= . . . ; | |

Sample Sheet: Configuring a “direct link” access point



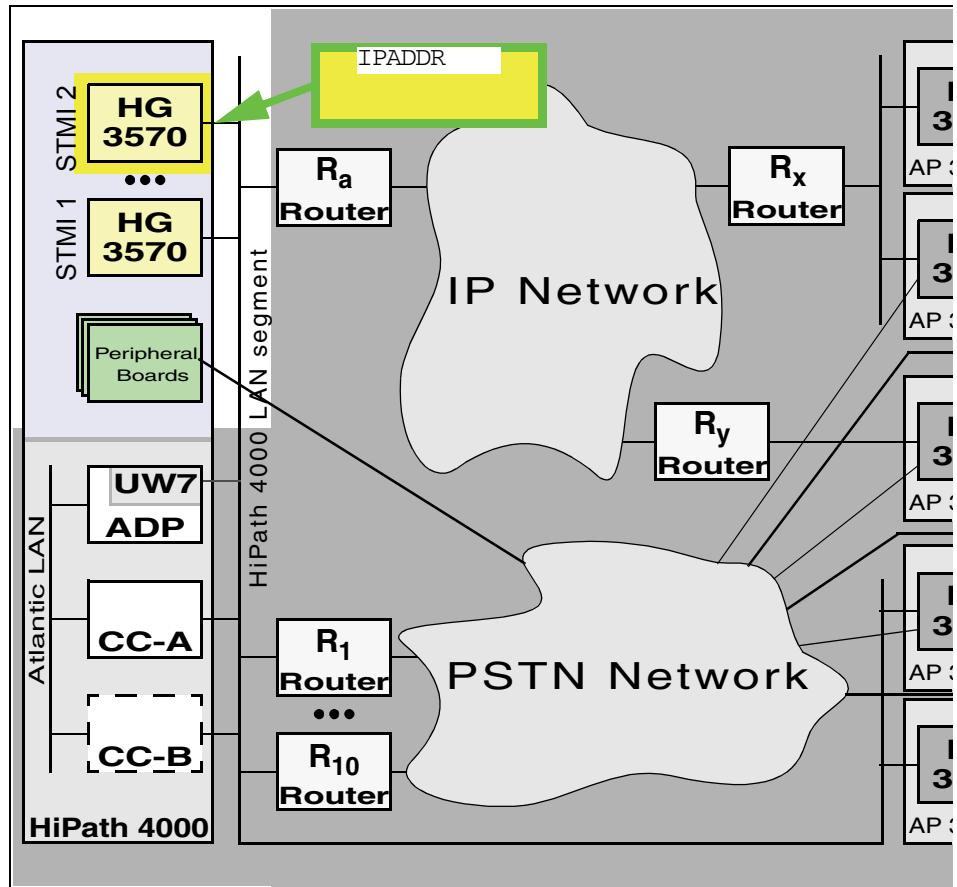
| | | |
|-----------|-------------------------|---|
| ADD-UCSU: | UNIT=AP, | LTU=17, |
| | LTPARTNO=Q2302-X10, | SRCGRP=1, |
| | FRMTYPE=INCH19, | CONNTYPE=APDL, |
| | LSRTADDR=192.168.1.17, | APRTADDR=192.168.1.254, |
| | LOCID=1, | LOCATION="MCH MACHTLFINGERSTR.1 GEB. 7202-111", |
| | PHONE=08972223456, | FAX=08972265432, |
| | PLCHECK=YES, | BCHLCNT=20, |
| | CONVLAW=NO; | |
| ADD-APRT: | TYPE=APNET, | LTU=17, |
| | APIPADDR=192.168.200.1, | NETMASK=255.255.255.252, |
| | TAIPADDR=192.168.200.2; | |

Spreadsheet: Configuring HiPath HG 3500 as HG3570 in the HiPath 4000 system



| | | |
|---------------|----------------|-------------------|
| ADD-BFDAT: | FCTBLK= , | FUNCTION=HG3570 , |
| | BRDBCHL= ; | |
| CHANGE-BFDAT: | CONFIG=CONT , | FCTBLK= , |
| | FUNCTION= , | BCHLCNT= ; |
| CHANGE-BFDAT: | CONFIG=OK , | FCTBLK= , |
| | ANSW= ; | |
| ADD-BCSU: | MTYPE=IPGW , | LTU= , |
| | SLOT= , | PARTNO=Q23 -X , |
| | FCTID= , | FCTBLK= , |
| | IPADR= . . . , | BCHL3570= ; |
| CHANGE-BCSU: | TYPE=HWYBDL , | LTU= , |
| | SLOT= , | PARTNO=Q23 -X , |
| | HWYBDL=A; | |

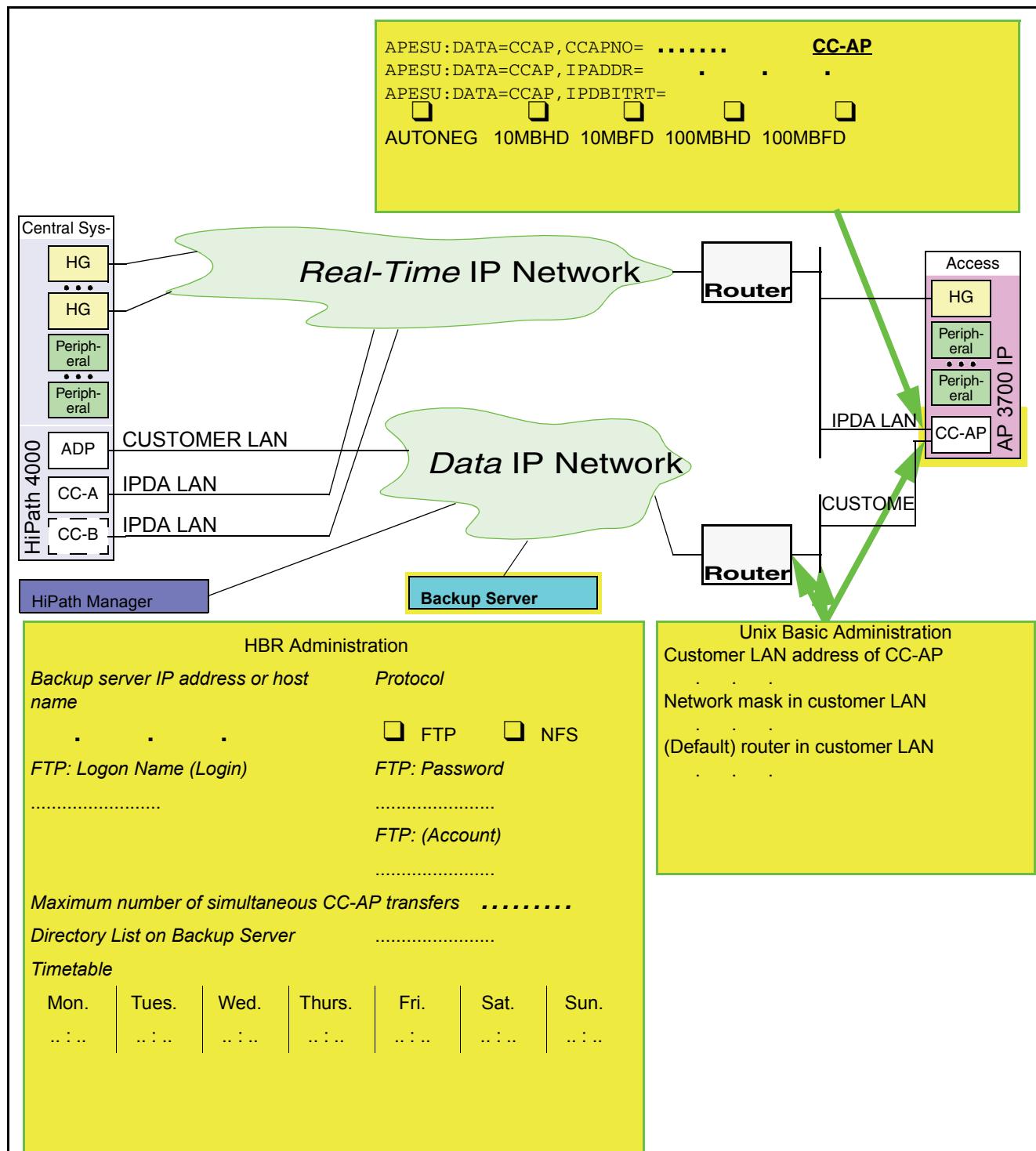
Sample Sheet: Configuring HiPath HG 3570 as HG3570 in the HiPath 4000 system



| | | |
|---------------|------------------------|------------------|
| ADD-BFDAT: | FCTBLK=1, | FUNCTION=HG3570, |
| | BRDBCHL=BCHL60&BCHL120 | |
| | ; | |
| CHANGE-BFDAT: | CONFIG=CONT, | FCTBLK=1, |
| | FUNCTION=HG3570, | BCHLCNT=40; |
| CHANGE-BFDAT: | CONFIG=OK, | FCTBLK=1, |
| | ANSW=YES; | |
| ADD-BCSU: | MTYPE=IPGW, | LTU=5, |
| | SLOT=91, | PARTNO=Q2316-X, |
| | FCTID=1, | FCTBLK=1, |
| | IPADR=192.168.1.11, | BCHL3570=40; |
| CHANGE-BCSU: | TYPE=HWYBDL, | LTU=5, |
| | SLOT=91, | PARTNO=Q2316-X, |
| | HWYBDL=A; | |

Spreadsheets - IPDA Configuration

AP Emergency spreadsheet: configuring a CC-AP



Two separate networks are shown in the spreadsheet for real-time or data communication. If one network is used for both communication types, both routers are identical.

AP Emergency spreadsheet: emergency group

9 LCT configuration

9.1 Configuring the PPP Connection to HG 3575 under Windows 2000

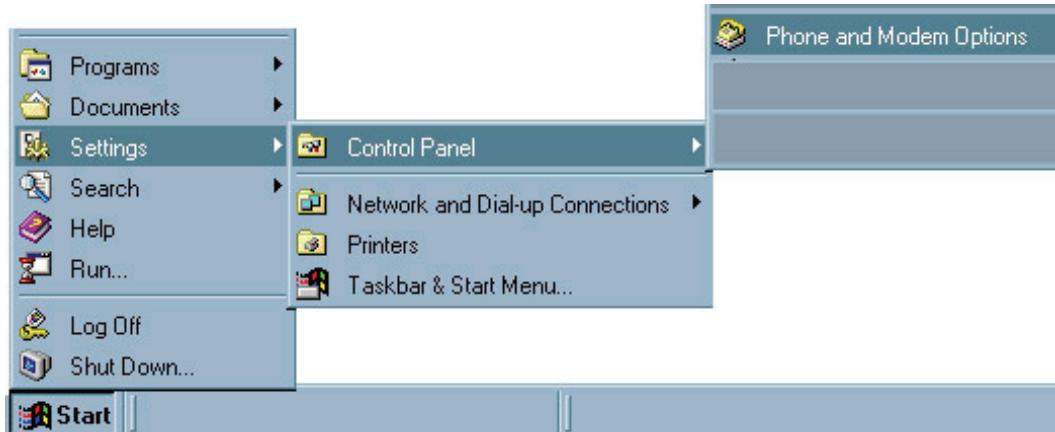
The installation takes place in two steps. First, the NULL modem must be configured (see Section 9.1.1, “Installing the NULL Modem”), and then the dial-up connection that uses the NULL modem (see Section 9.1.2, “Installing the PPP Connection”).

The PPP connection here is independent of “HiPath 4000 Expert Access”; however, it presupposes the installation of “HiPath 4000 Expert Access” because a necessary connection profile is installed during “HiPath 4000 Expert Access” installation. The NULL modem should have been installed with “HiPath 4000 Expert Access” as well.

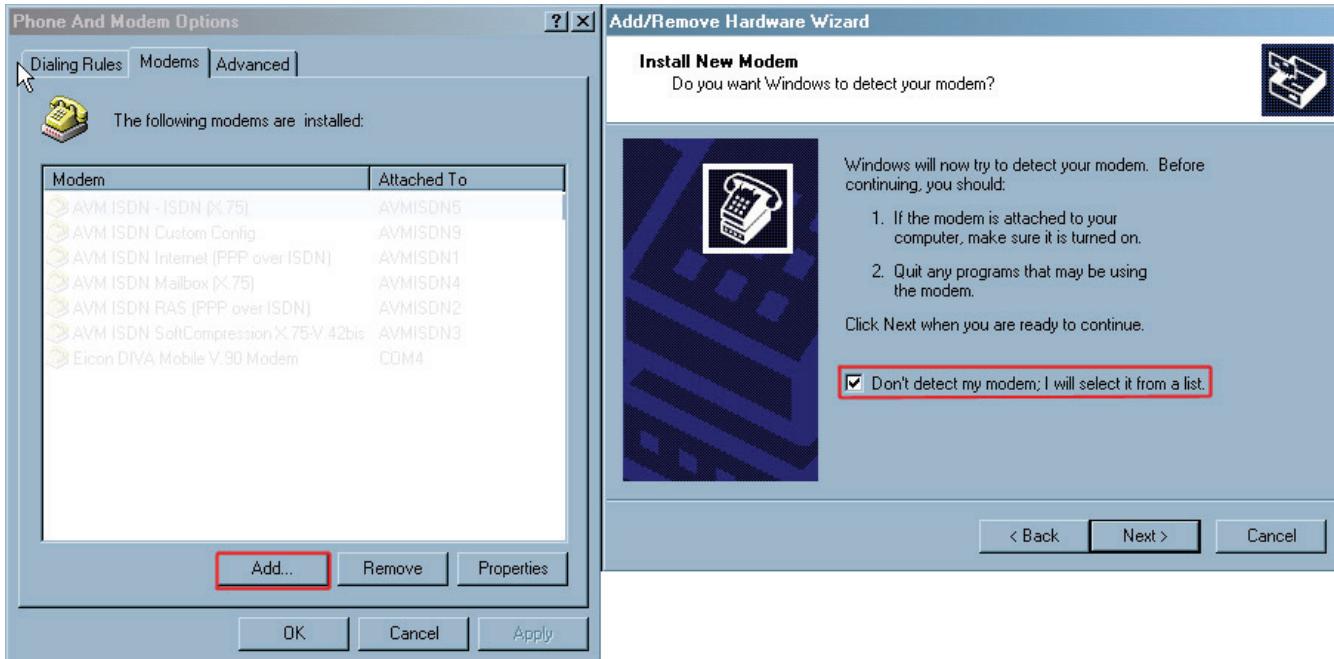
9.1.1 Installing the NULL Modem

The NULL modem for the PPP connection can be configured via

-> «Settings» -> «Control Panel» -> «Phone and Modem Options».



The following dialog appears:



If the *Generic NULL Modem* is not in the list of selections, it needs to be added.

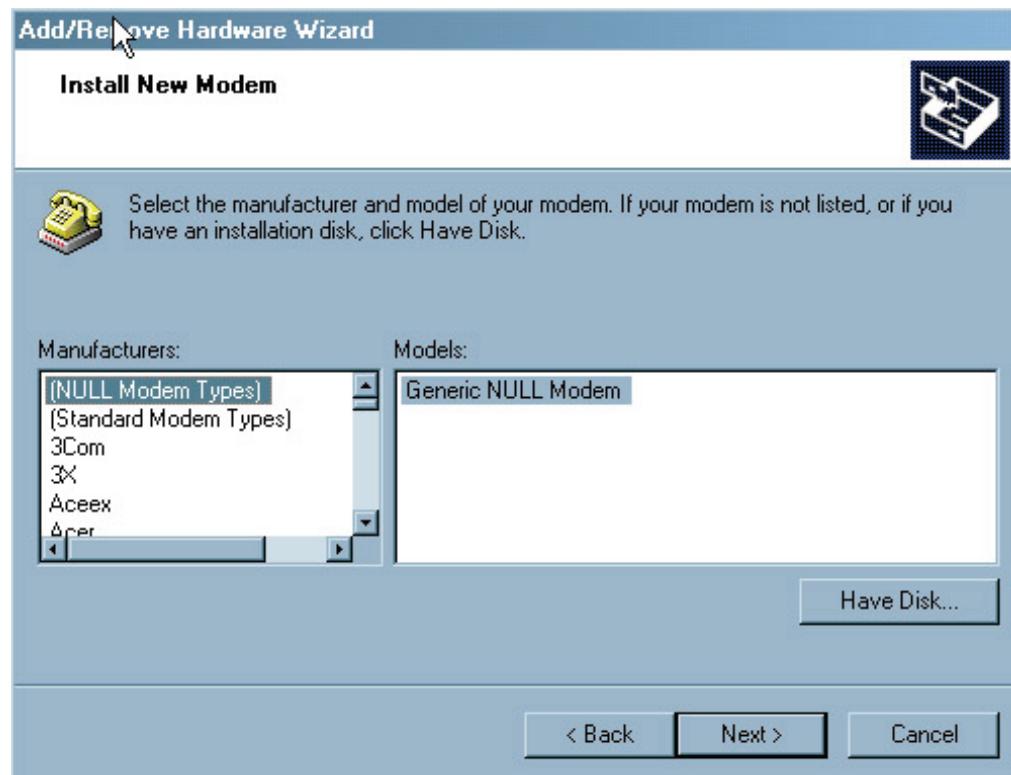
If it is already listed, proceed with Installing the PPP Connection.

After selecting **Add ...** you will see the Add/Remove Hardware Wizard.

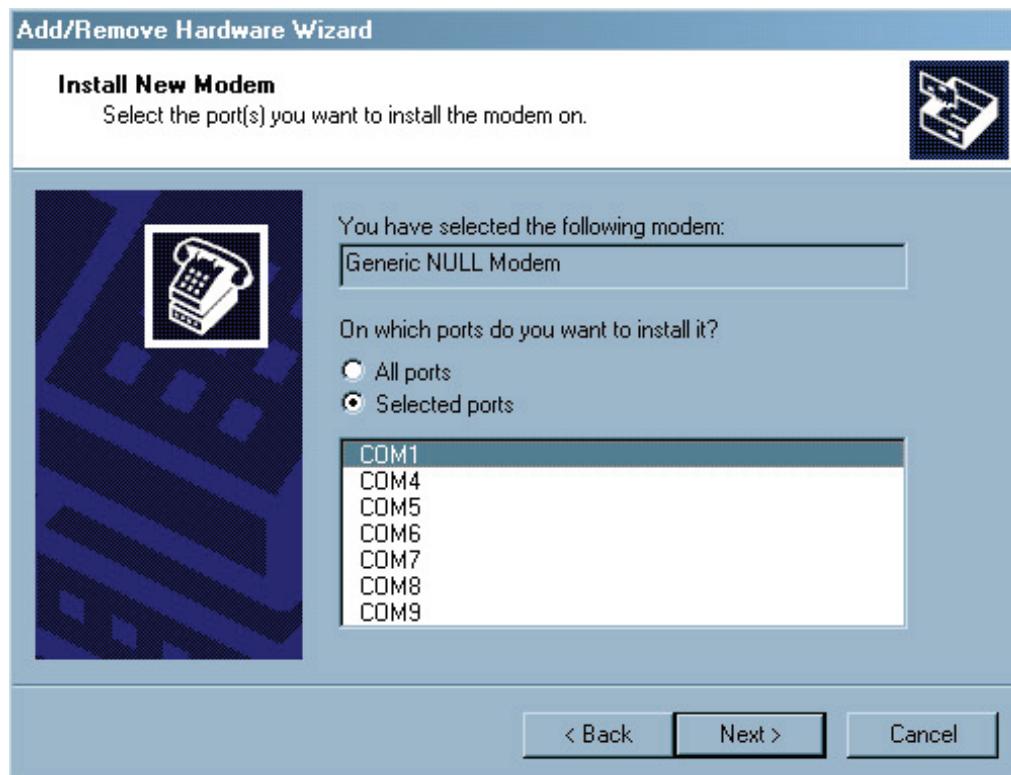
In the start window for the Hardware Wizard, activate the checkbox «**Don't detect my modem; I will select it from a list.**». Confirm your selection with **Next**.

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000



For the manufacturer, select «(NULL Modem Types)» from the selection list; for the model, select «Generic NULL Modem». Confirm your selection with **Next**.



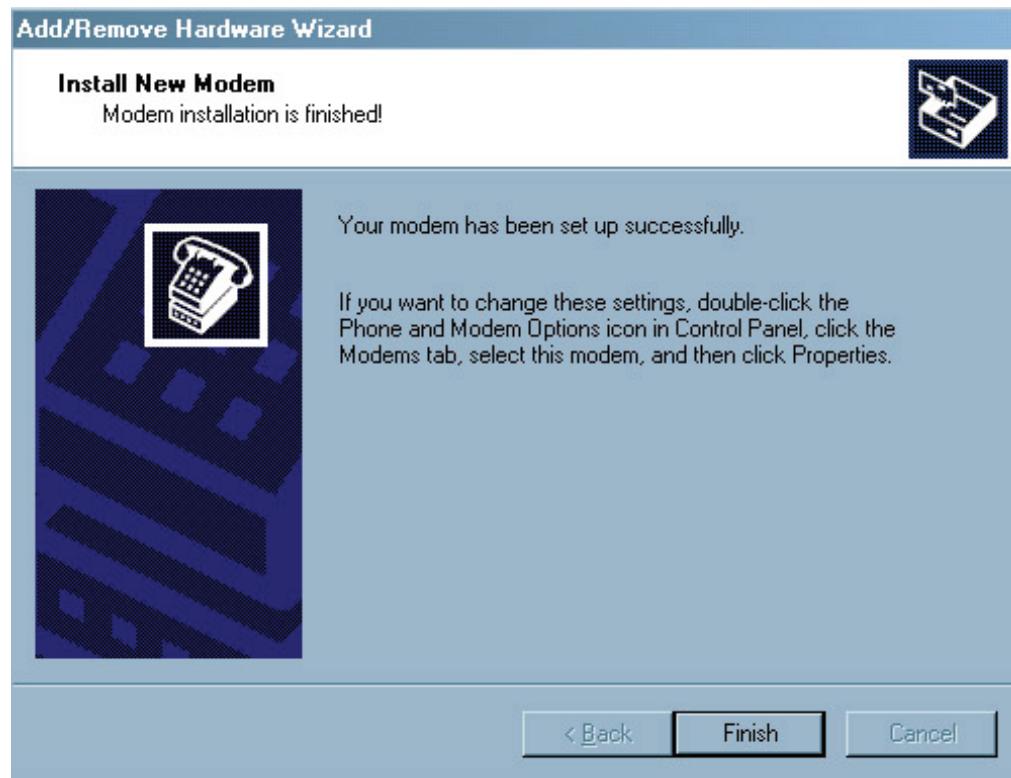
Next, select the port on which the *Generic NULL Modem* should be activated. Normally, this is «COM1». Confirm your selection with **Next**.



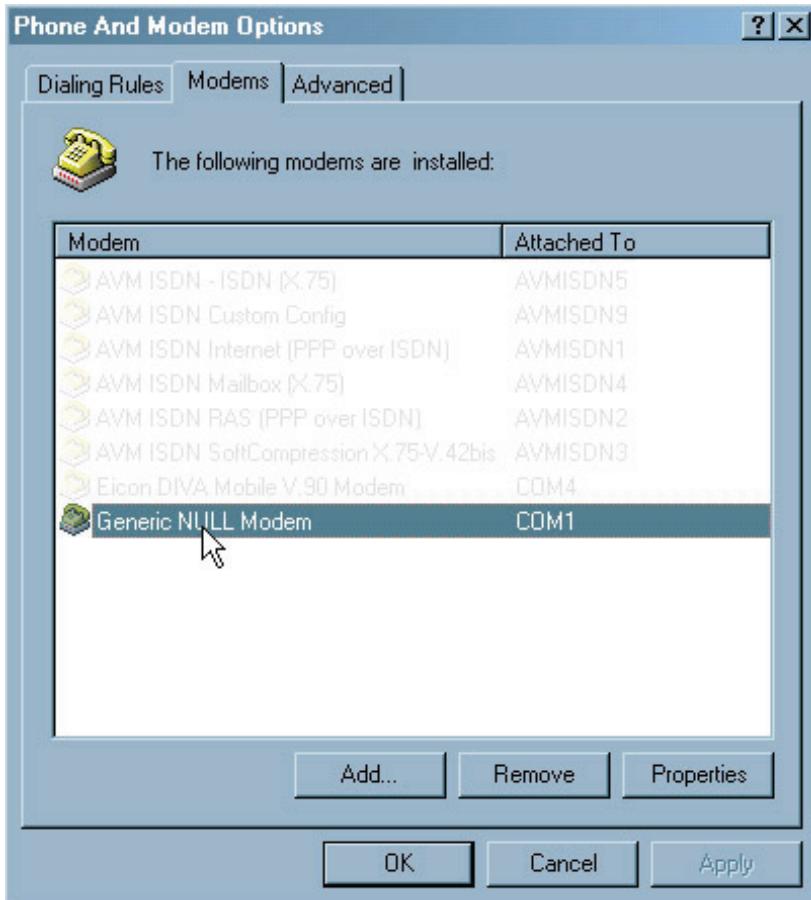
LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000

There is no digital signature available for the *Generic NULL Modem* driver. Windows 2000 displays the following dialog to alert you to this fact. By selecting **Yes**, you can continue with the installation.



The installation of the *Generic NULL Modem* is now complete. Confirm with **Finish**.



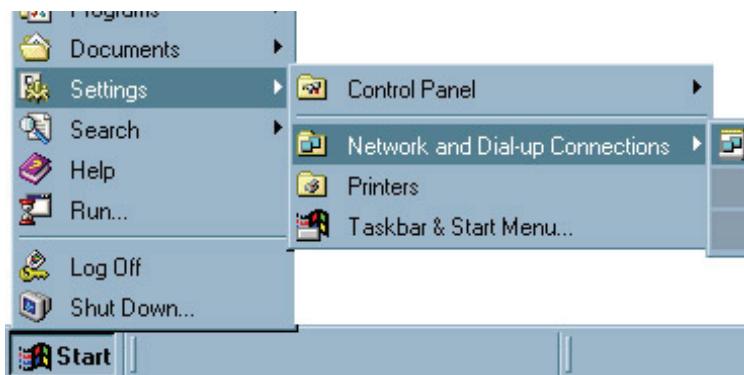
The *Generic NULL Modem* is now located in the list of installed modems. Please select the NULL modem and confirm your selection with **OK**.

LCT configuration

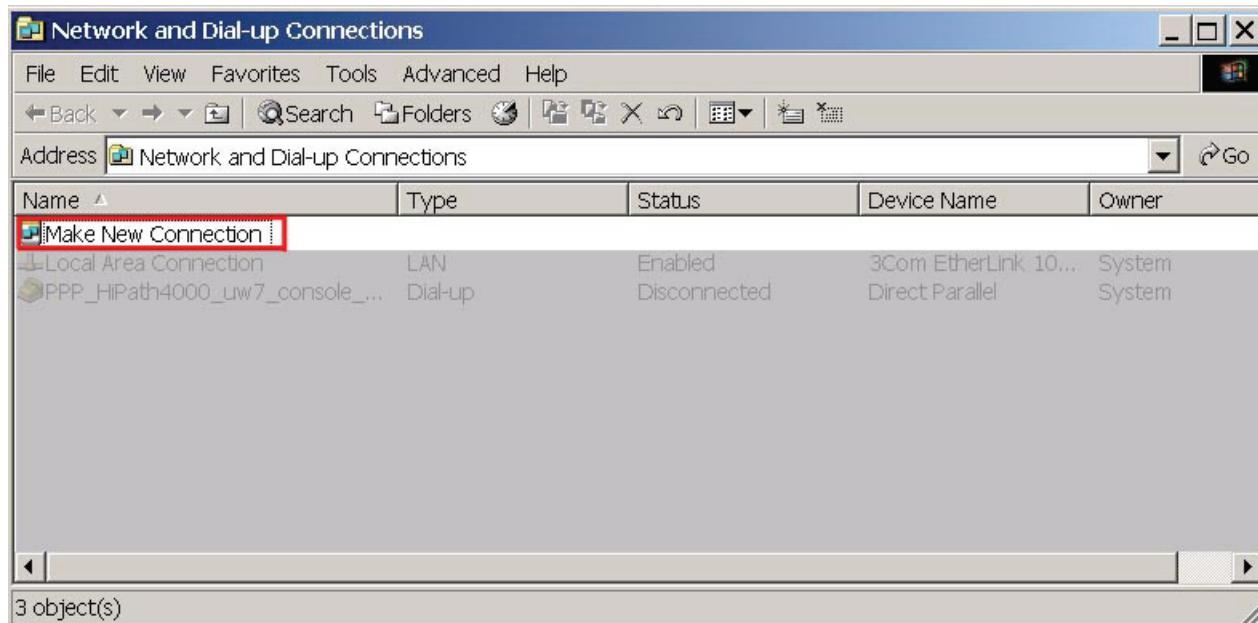
Configuring the PPP Connection to HG 3575 under Windows 2000

9.1.2 Installing the PPP Connection

The new PPP connection can be configured via -> «Settings» -> «Network and Dial-up Connections»



The following dialog appears.



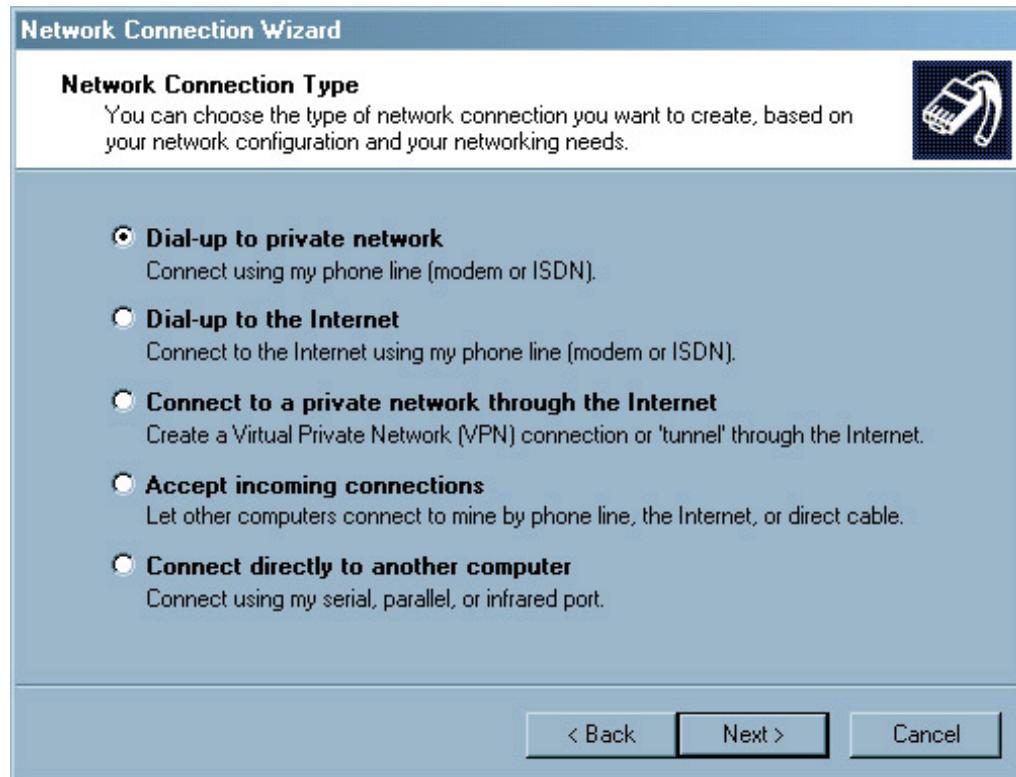
In the list of configured network and dial-up connections, please select «Create New Connection». The Network Connection Wizard opens.



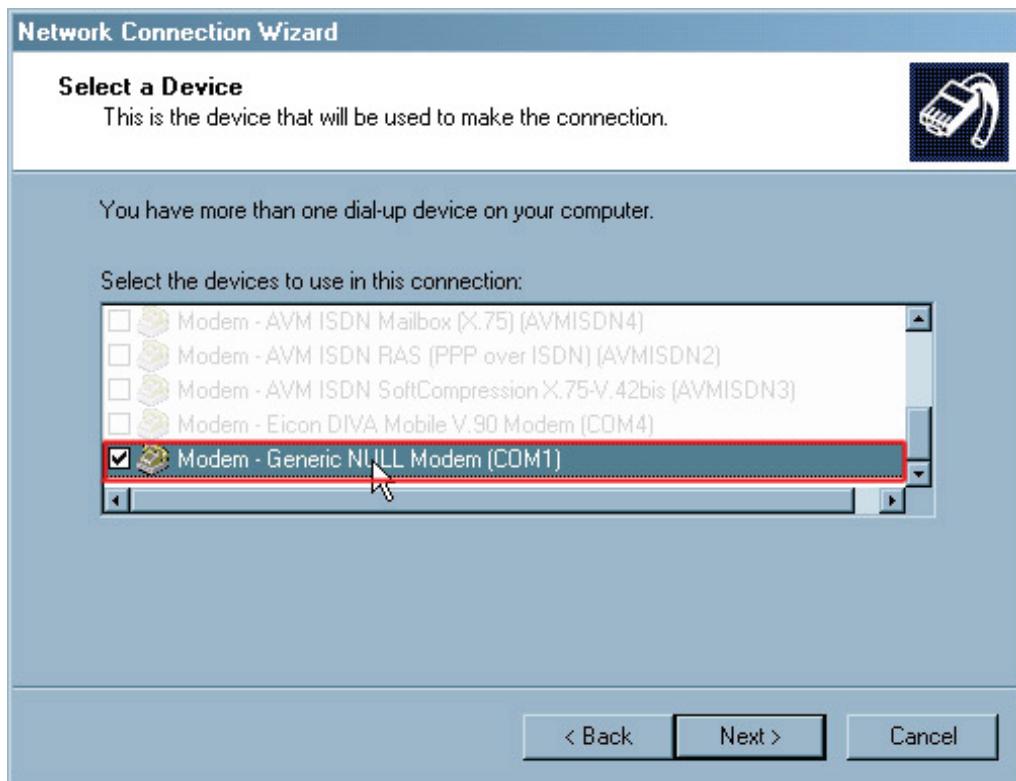
Confirm with **Next**.

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000



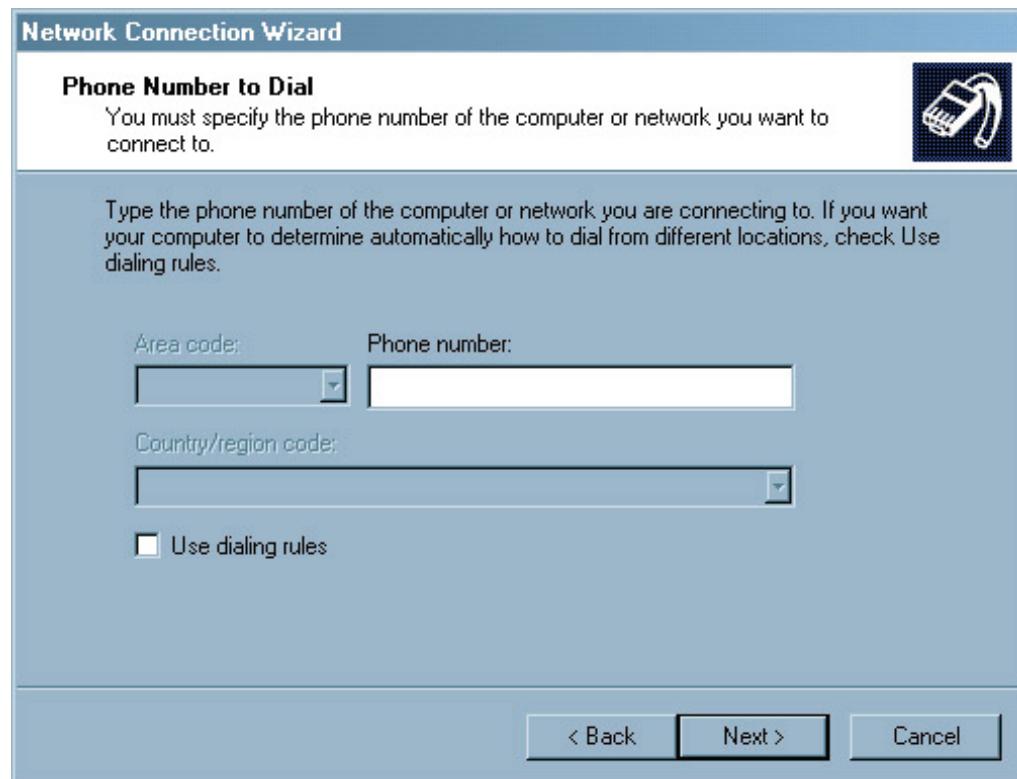
First, the network connection type must be selected. Select «Dial up to a private network». If your PC does not support this setting, you need further administration privileges. Confirm your selection with **Next**.



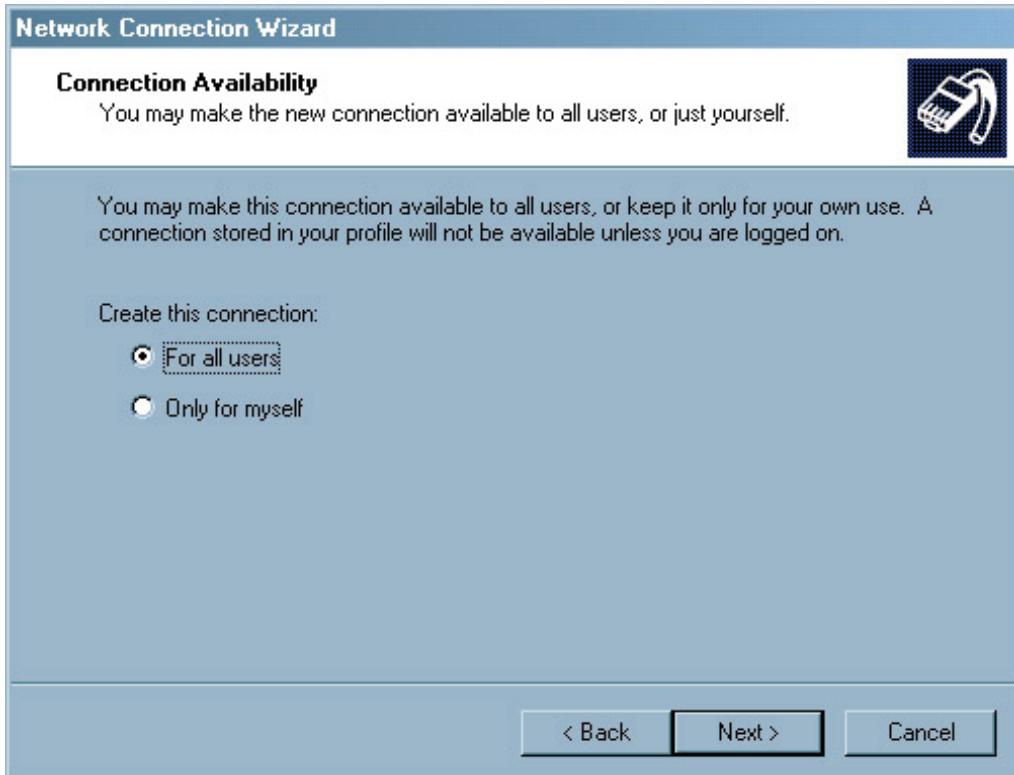
Now select the device that will be used for connecting. This should be «Modem – Generic NULL Modem (COM 1)». Confirm your selection with **Next**.

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000



Next, you are asked to supply the phone number to be dialed. The NULL modem does not require a number. Confirm with **Next**.



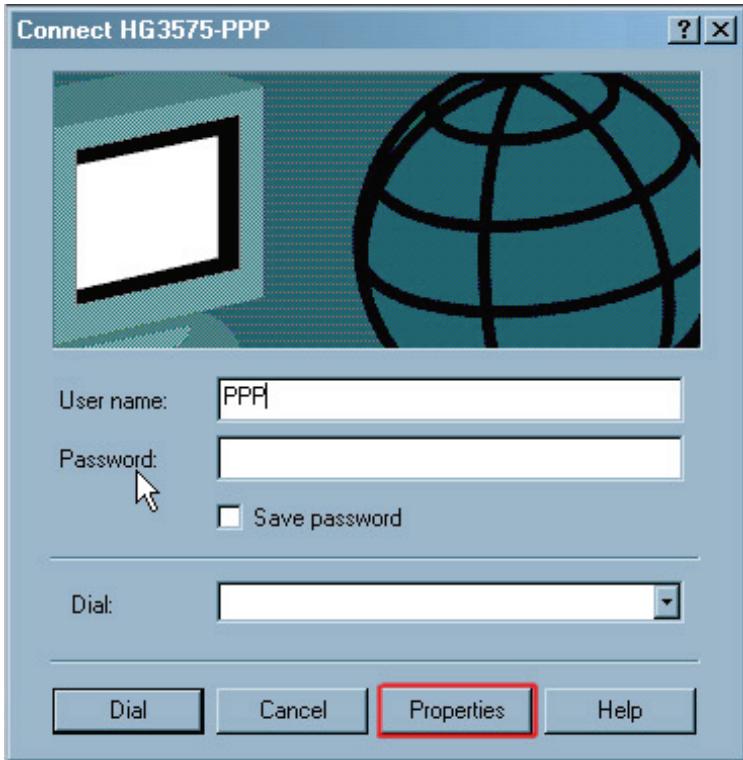
In the Connection Availability window you can define whether this connection is available for all PC users or only for yourself. Confirm your selection with **Next**.

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000



In the final window of the Network Connection Wizard, enter a name for the configured connection, for example, «HG3575-PPP» and confirm with **Finish**.



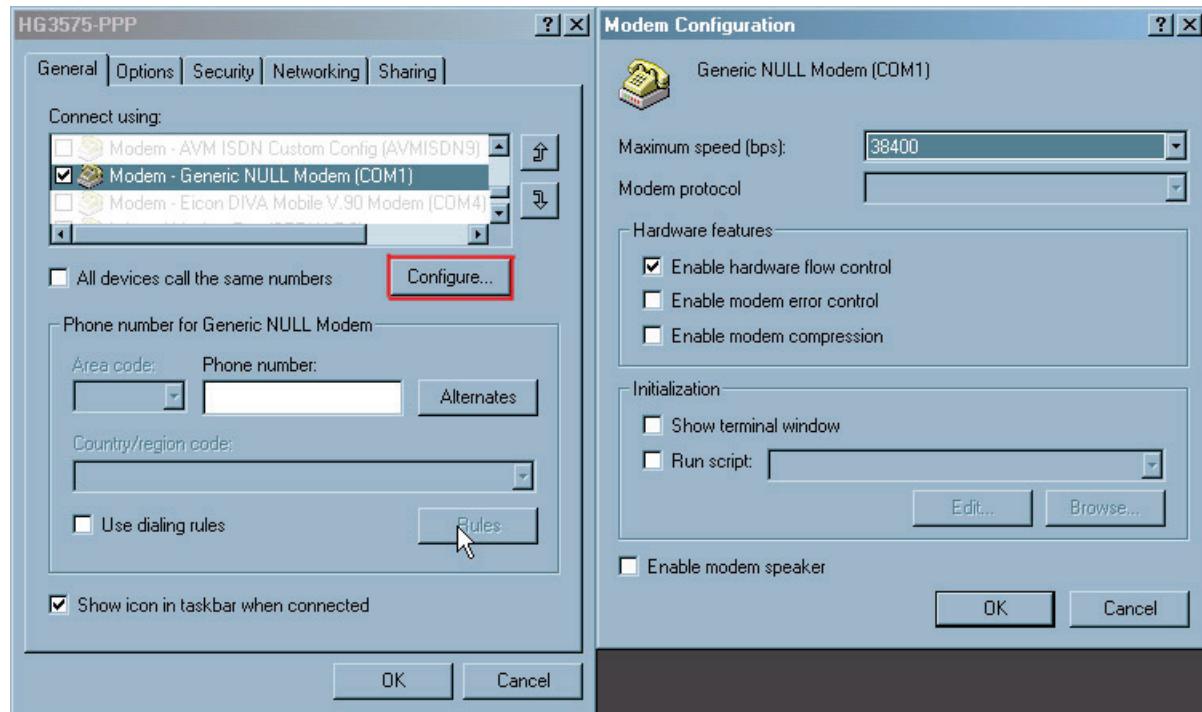
You are now presented with the connection's "Logon" window.

If this window does not automatically appear after completing the Network Connection Wizard, select the newly configured connection from the network connections list with the right mouse button and from the context menu select «Properties».

User name (default: «PPP») and password (default: none, leave field empty) should be entered here. Substantial parts of the installation are only accessible via the **Properties** button.

LCT configuration

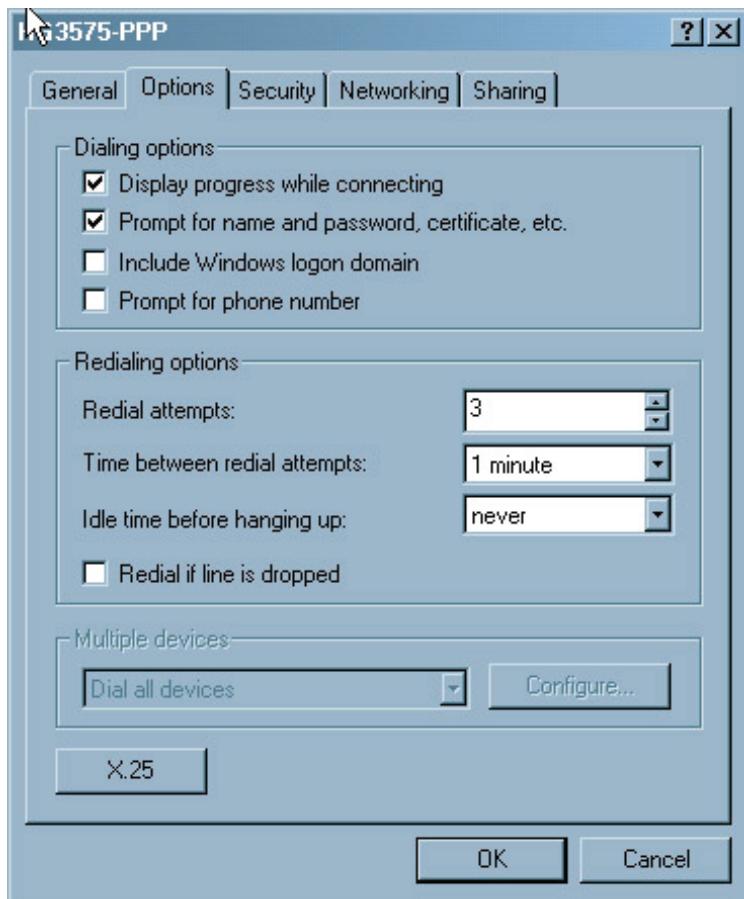
Configuring the PPP Connection to HG 3575 under Windows 2000



Under «Properties» - «General», you are presented again with «Connect using:» «Generic NULL Modem». No other additional devices can be selected here. The window «Modem Configuration» can be opened via the **Configure...** button.

This is where «Maximum speed (bps) : » is configured to «38400» and «Enable hardware flow control» is activated. All further options remain inactive. Make all configurations exactly as illustrated in the figure.

Confirm with **OK**.



Next, you should select «Properties» - «Options».

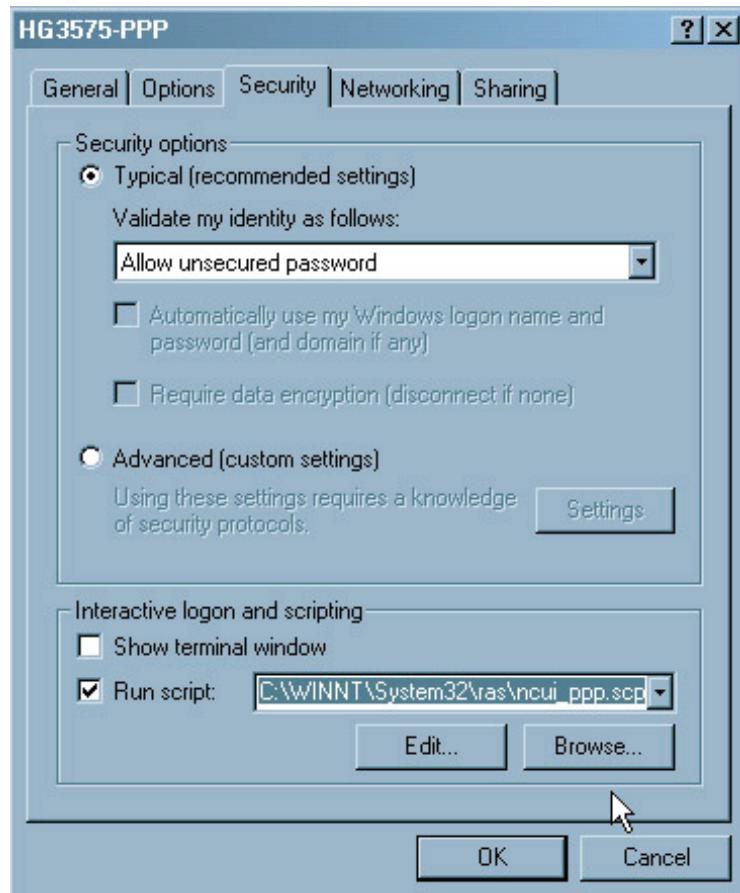
The options «Display progress while connecting» and «Prompt for name and password, certificate, etc. » are activated in this tab.

The redialing options are set to default values; all further options remain inactive.

Confirm with **OK**.

LCT configuration

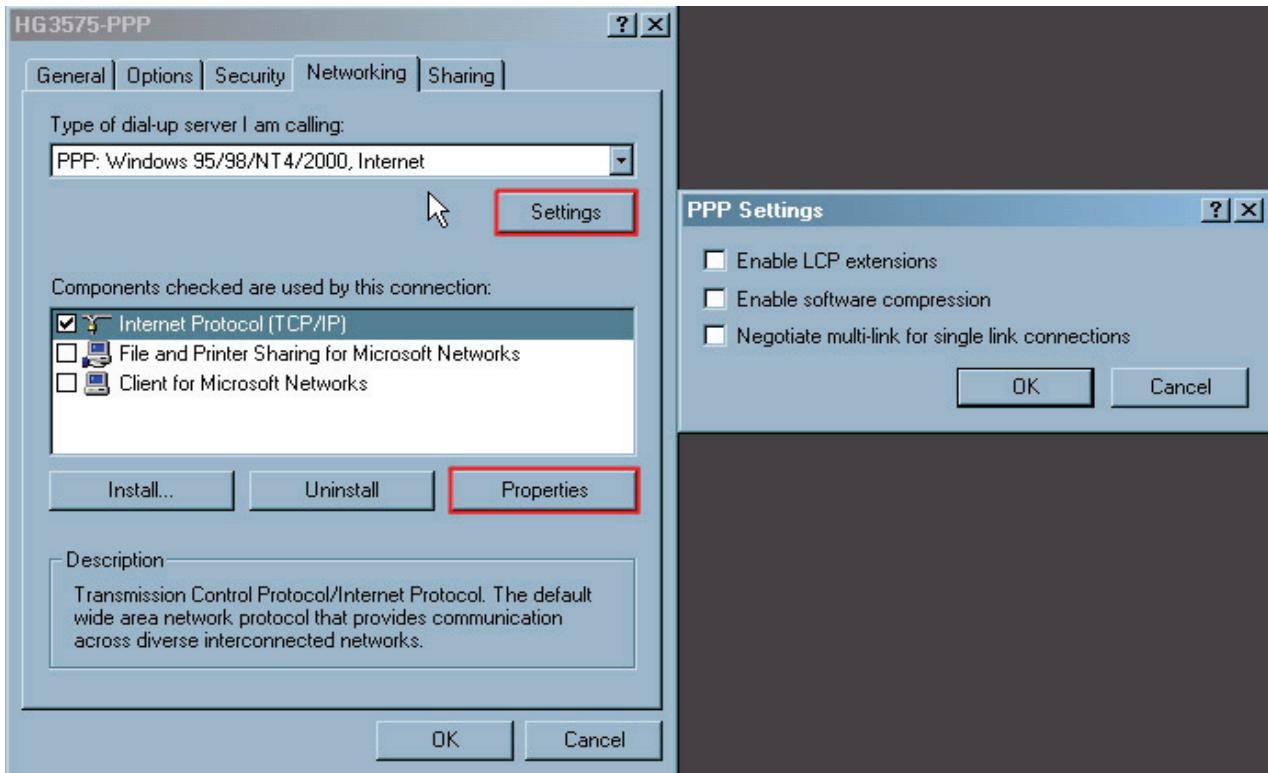
Configuring the PPP Connection to HG 3575 under Windows 2000



Under «Properties» - «Security», the «Security options» should be set to «Typical (recommended settings)» and «Allow unsecured password» should be selected.

Under «Interactive logon and scripting», activate the «Run script :» checkbox and select the script «C : \WINNT\System32\ras\ncui_ppp .scp», which was installed on your PC along with "HiPath 4000 Expert Access".

All further options remain inactive. Confirm this configuration with **OK**.



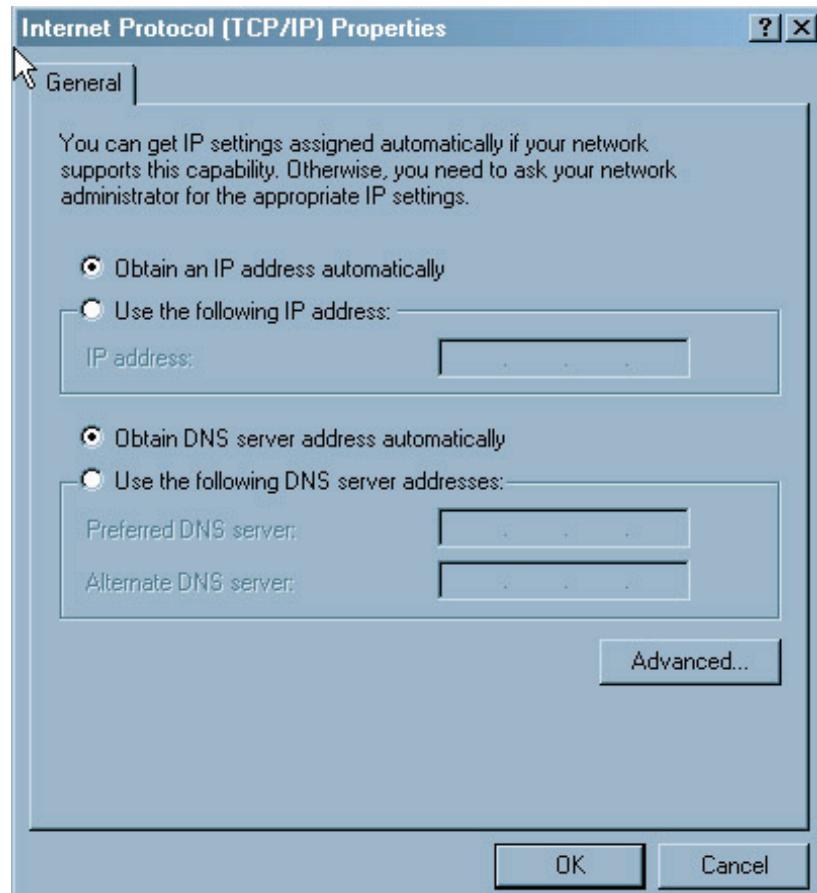
Please select «Properties» - «Networking». The «Type of dial-up server I am calling:» needs to be set to «PPP: Windows 95/98/NT4/2000, Internet».

Clicking the **Settings** button will open the «PPP Settings» dialog, in which all options must be deactivated. Please confirm your selection with **OK**.

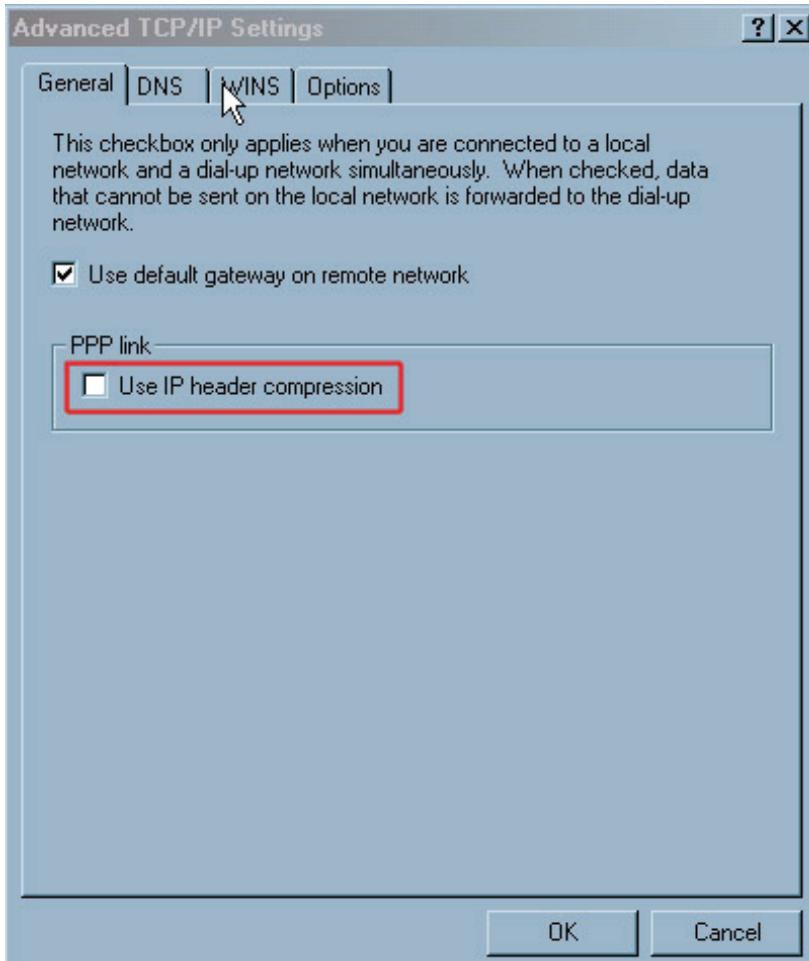
Only the «Internet Protocol (TCP/IP)» needs to be active for the connection. Select this entry and, via the **Properties** button, proceed to the «Internet Protocol (TCP/IP) Properties» window.

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows 2000



Under «Internet Protocol (TCP/IP) Properties», make sure the options «Obtain IP address automatically» and «Obtain DNS server address automatically» are selected. Crucial settings are located in «Advanced TCP/IP Settings», which you can access via the **Advanced...** button.



Under «Advanced TCP/IP Settings», activate the checkbox «Use default gateway on remote network» and deactivate the checkbox «Use IP header compression». - Confirm your selection with **OK**. This takes you back to the «Internet Protocol (TCP/IP) Properties» window. By clicking on the **OK** button in this dialog, you are returned to the PPP connection's properties dialog, which can be closed by selecting **OK**.

This concludes configuration of the PPP connection of the TAP to the HG 3575 (NCUI).

9.2 Configuring the PPP Connection to HG 3575 under Windows XP

The installation takes place in two steps. First, the NULL modem must be configured (see Section 9.2.1, “Installing the NULL Modem”), and then the dial-up connection that uses the NULL modem (see Section 9.2.2, “Installing the PPP Connection”).

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows XP

The PPP connection here is independent of "HiPath 4000 Expert Access"; however, it presupposes the installation of "HiPath 4000 Expert Access" because a necessary connection profile is installed during "HiPath 4000 Expert Access" installation. The NULL modem should have been installed with "HiPath 4000 Expert Access" as well.

9.2.1 Installing the NULL Modem

- The NULL modem for the PPP connection can be configured via **Settings > Control Panel** and double clicking the **Phone and Modem Options** icon.

The **Phone and Modem Options** dialog appears.

If the Generic NULLModem is not in the list of selections, it needs to be added, select **Add...**.

If it is already listed, proceed with Installing the PPP Connection.

- Do you want windows to detect your modem?

After selecting **Add..** the **Add Hardware Wizard** is displayed.

In the start window for the Add Hardware Wizard, activate the checkbox **Don't detect my modem; I will select it from a list..** Confirm your selection with **Next.**

- Select the manufacturer and the model of your modem.

For the **Manufacturer**, select **(NULL Modem Types)** from the selection list; for the **Model**, select **Generic NULL Modem**. Confirm your selection with **Next.**

- Select the port(s) you want to install the modem on.

Now select the port on which the Generic NULL Modem should be activated. Normally, this is **COM1**. Confirm your selection with **Next.**

- If the compatibility of the Generic NULL Modem driver cannot be verified, Windows XP displays the following dialog to alert you to this fact. By selecting **Continue Anyway**, you can continue with the installation.



- Installation is finished.

The installation of the Generic NULLModem is now complete. Confirm with **Finish**.

- Phoe and Modem Options

The Generic NULLModem is now located in the list of installed modems. Please select the NULL modem and confirm your selection with **OK**.

9.2.2 Installing the PPP Connection

- The new PPP connection can be configured via **Settings > Control Panel** and double clicking the **Network Connections** icon.

The **Newtork Connections** dialog appears.

- In the list of configured network and dial-up connections, please select **New Connection Wizard**. The **Network Connection Wizard** opens.

- To continue select **Next**.

- Network Connection Type

First, the network connection type must be selected. Select **Connect to the network at my workplace**. And confirm with with **Next**.

- Network Connection

Select **Dial-up connection** as network connection. Confirm your selection with **Next**.

- Connection Name

In this window enter the name for the connection, e.g. **HG3575-PPP**. Confirm with **Next**.

- Select a Device

Now select the device that will be used for connecting. This should be **Modem - Generic NULL Modem (COM 1)**. Confirm your selection with **Next**.

- Phone Number to Dial

Now you are asked to supply the phone number to be dialed. The NULL modem does not require a number. Confirm with **Next**.

- Smart Cards

Select wether to use your smart card for logging on. Confirm your selection with **Next**.

- Connection Availability

In the **Connection Availability** window you can define whether this connection is available for all PC users or only for yourself. Confirm your selection with **Next**.

- Completing the NEw Connection Wizard

LCT configuration

Configuring the PPP Connection to HG 3575 under Windows XP

This is the final window of the **Network Connection Wizard**. Complete the **Connection Wizard** by pressing **Finish**.

- Connection log on window (e.g Connect HG3575-PPP)

The connection Logon window appears.

If this window does not automatically appear after completing the **Network Connection Wizard**, select the newly configured connection from the network connections list with the right mouse button and select **Properties** from the context menu.

User name (default: **PPP**) and password (default: none, leave field empty) should be entered here. Substantial parts of the installation are only accessible via the **Properties** button.

The HG3575-PPP properties dialog appears.

- Tab sheet **General**

Connect using: Generic NULL Modem. No other devices can be selected here. The **Modem Configuration** window can be opened via the **Configure...** button.

In the Modem Configuration window the **Maximum speed (bps)** is set to **38400** and the check box **Enable hardware flow control** is activated. All further options remain inactive.

Confirm with **OK**.

- Tab sheet **Options**

Dialing options: Activate the options **Display progress while connecting** and **Prompt for name and password, certificate, etc..**

Don't change the **Redialing options**. The default values are correct.

Confirm with **OK**.

- Tab sheet **Security**

Security options: Select **Typical (recommended settings)** and select from the drop down list **Allow unsecured password**.

Interactive logon and scripting: Activate the **Run script:** checkbox and select the script **C:\WINNT\System32\ras\ncui_ppp.scp**, which was installed on your PC with **HiPath 4000 Expert Access**.

Confirm this configuration with **OK**.

- Tab sheet **Networking**

The **Type of dial-up server I am calling:** needs to be set to **PPP: Windows 95/98/ NT4/2000, Internet.**

Clicking the **Settings** button the "PPP Settings" dialog will open. In this dialog all options must be deactivated. Please confirm your selection with **OK**.

Select the **Internet Protocol (TCP/IP)** entry. Select this entry and click on the **Properties** button to proceed.

In the **Internet Protocol (TCP/IP) Properties** window, make sure the options **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

Now click on the **Advanced...** button. The **Advanced TCP/IP Settings** window appears. Activate the checkbox **Use default gateway on remote network** and deactivate the checkbox **Use IP header compression**.

Confirm your selection with **OK**. This takes you back to the **Internet Protocol (TCP/IP) Properties** window. By clicking on the **OK** button in this dialog, you are returned to the PPP connection's properties dialog, which can be closed by selecting **OK**.

9.3 Notes on Using the PPP Connection

- After a successful PPP connection, the HiPath 4000 Assistant on the HiPath 4000's UW7 system can be accessed by entering the following URL in the address field of your browser: "<http://<UW7 IP Address>>". The **<UW7 IP Address>** should be replaced by the IP address of the UW7 LAN connection.
- If LCT access is requested from the access point on the central system, the UW7 LAN interface **must** be located in the HiPath 4000 LAN segment (see Section 4.1, "Configuring the HiPath 4000 LAN Segment", on page 4-38).
- Routing to the access points (which will be configured for CC-A or CC-B) also needs to be configured in UW7.
- Before starting a PPP connection from the LCT to the central system at the access point, a preliminary terminal login may need to be ended from the command line (CLI). [logout].

10 Information for network administrators

10.1 Central Processor

Every central processor receives an additional LAN interface for controlling access points when an IPDA system is installed.

| | |
|-----------------------------|---|
| PHY | 10/100 Base T - autosensing or can be permanently set |
| MAC address | Permanently programmed on the interface card, ->sticker |
| IP address | Configured in the HiPath 4000 system, can be set |
| IEEE 802.1 p/q VLAN tagging | Configurable; priority bits are always set when active. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the HiPath 4000 system. |
| TOS/DiffServ | The six highest bits in the TOS byte can be set. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. Configuration in the HiPath 4000 system. |
| Protocols/ports | See Chapter 20, “IP Ports” in the document “HiPath Gateways HG 3500 and HG 3575”. |
| Routing | A host route that is configured in the HiPath 4000 system is used to every access point. No default route. |
| Firewall | The central processor only allows connections to addresses that it knows, i.e. access points or assigned service PCs. |
| Number of connections | Up to 166 TCP/IP connections (two per access point) |

In large systems, two redundant central processors are installed, one of which is always active. Every processor has its own IP network connection with its own IP and MAC address. PHY is active in the standby processor. However, the standby processor does not receive and send packets.

10.2 HG 3500 Voice Gateway

These boards are installed in the HiPath 4000 central system. A maximum of 83 HG 3500 boards can be configured in a system.

| | |
|-------------|---|
| PHY | 10/100 Base T - autosensing or can be permanently set |
| MAC address | Permanently programmed on the board, ->sticker |

| | |
|-----------------------------|---|
| IP address | Configured in the 4000 system, can be set. It must be in the same network segment as the central processor. The address is assigned to the slot in the system. When a board is exchanged, the new one automatically adopts the IP address. |
| IEEE 802.1 p/q VLAN tagging | Configurable; priority bits are always set when active. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the HiPath 4000 system. |
| TOS/DiffServ | The six highest bits in the TOS byte can be set. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. Configuration in the HiPath 4000 system. |
| Protocols/ports | See Chapter 20, “IP Ports” in the document “HiPath Gateways HG 3500 and HG 3575”. |
| Routing | Routing table configured in the HiPath 4000 system with a default route and up to eight additional routes. Routing is identical for all HG 3500s in the system. |
| Number of connections | Up to 30/60/120 RTP and RTCP connections to any access points, depending on the hardware used. Connection setup controlled completely from HiPath 4000. H.323 Fast Connect for direct media connections outside the IPDA gateway network, no gatekeeper necessary. See Section 6.2, “Load Calculation for a HG 3500” for connection bandwidths. |

10.3 Access Points with HG 3575

An HG 3575 is used as the central board for each access point. Access points are only connected to the central system via IP. A maximum of 83 access points can be configured in a system.

As regards addresses, a distinction must be made between “networked” and “direct link” access points.

“Networked” access points are in a different network segment to the central system and can therefore only be reached via a router.

“Direct Link” access points are connected in the same network segment as the central system.

The HiPath 4000 system is used for configuring addresses and the port settings. The access point is stored locally. The parameters must be set locally for initial startup.

Information for network administrators

Access Points with HG 3575

| | |
|-----------------------|---|
| PHY | 10/100 Base T - autosensing or can be permanently set |
| MAC address | Permanently programmed on the board, ->sticker |
| IP addresses | See below |
| IEEE 802.1 p/q | Configurable; priority bits are always set when active. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. |
| VLAN tagging | The VLAN ID can be set. Configuration in the HiPath 4000 system. |
| TOS/DiffServ | The six highest bits in the TOS byte can be set. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. Configuration in the HiPath 4000 system. |
| Protocols/ports | See Chapter 20, “IP Ports” in the document “HiPath Gateways HG 3500 and HG 3575”. |
| Routing | Routing table configured in the HiPath 4000 system with a default route and up to eight additional routes. Routing can be individually set for the access point. |
| Number of connections | <p>Up to 30/60/120 RTP and RTCP connections to any HG 3500 or access points.</p> <p>Connection setup controlled completely from HiPath 4000.</p> <p>H.323 Fast Connect for direct media connections outside the IPDA gateway network, no gatekeeper necessary.</p> <p>Up to two TCP/IP connections to the central processor.</p> <p>When using AP Emergency features and a TCP/IP connection to the survivability unit.</p> <p>See Section 6.1, “Load Calculation for Access Points” for connection bandwidths.</p> |

IP addresses for “networked“ access points:

| | |
|---|--|
| IP address of the access point | For signaling, payload, SNMP, FTP, Telnet. See Figure 21 “Difference between “networked“ and “direct link“ access point” on page 4-57 Address must be routed in the network. |
| IP address for service PC | Optional. PC is connected to the access point via a serial interface. Uses PPP between PC and AP. Operates in the network under this address. The destinations are the central processor (for ping) and the UW7 administration computer for administering the HiPath 4000 system. Address must be routed in the network. |
| IP address for signaling survivability | see Section 4.5, “Configuring Signaling Survivability”, on page 4-112. This address remains invisible in the LAN as it is only used for the PPP connection between the survivability router and modem connection of the access point. This address is assigned indirectly by configuring the network address for the virtual survivability network (PPP via ISDN). Only a “private“ address such as 192.168.x.0 should be used here. |

Information for network administrators

Access Points with HG 3575

IP address for “direct link“ access points:

| | |
|---|---|
| IP address of the access point | For payload, SNMP, FTP, Telnet, however not for signaling. See Figure 21 “Difference between “networked“ and “direct link“ access point” on page 4-57. Address must be in the same network segment as the central processor. Address must be routed in the network. |
| IP address for signaling | The signaling connection between the central processor and the access point must pass via a router. See Figure 21 “Difference between “networked“ and “direct link“ access point” on page 4-57. If the LAN connection fails, the current TCP connection is rerouted for signaling survivability. This can only be performed by changing the router whereas the destination address remains the same. An internal router which routes between the access point IP address and the internal address of the signaling instance is therefore used for “direct link“ access points. The IP address for signaling must be in a separate “private“ network segment. It is visible in the LAN (using a sniffer) as the destination address of the signaling packet. However, as signaling packets are routed exclusively from the central processor to the access point IP address via the host route, no router needs to/must route this address in the LAN. Only a “private“ address such as 192.168.x.0 should be used here. |
| IP address for service PC | Optional. PC is connected to the access point via a serial interface. Uses PPP between PC and AP. Operates in the network under this address. The destinations are the central processor (for ping) and the UW7 administration computer for administering the HiPath 4000 system. Address must be in the same internal network as the access point signaling instance (see above). |
| IP address for signaling survivability | see Section 4.5, “Configuring Signaling Survivability”, on page 4-112. This address remains invisible in the LAN as it is only used for the PPP connection between the survivability router and modem connection of the access point. This address is assigned indirectly by configuring the network address for the virtual survivability network (PPP via ISDN). Only a “private“ address such as 192.168.x.0 should be used here. |

10.4 Survivability Unit for AP Emergency

The survivability unit integrates a control processor in an access point. A maximum of 83 survivability units can be integrated in the system with the maximum 83 access points per system.

The survivability unit processor requires 2 LAN connections in the IP network.

Detailed information can be found in Section 3.4, “AP 3700 IP with Survivability Unit in the Customer LAN”, on page 3-34.

An “IPDA“ interface is required for the signaling connection with the allocated access points.

| | |
|-----------------------------|---|
| PHY | 10/100 Base T - autosensing or can be permanently set |
| MAC address | Permanently programmed ->sticker (the higher of the two addresses) |
| IP address | Configured in the HiPath 4000 system, can be set |
| IEEE 802.1 p/q VLAN tagging | Configurable; priority bits are always set when active. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. The VLAN ID can be set. Configuration in the HiPath 4000 system. |
| TOS/DiffServ | The six highest bits in the TOS byte can be set. See Table 2 “TOS values” in document “HiPath Gateways HG 3500 and HG 3575”. Configuration in the HiPath 4000 system. |
| Protocols/ports | See Chapter 20, “IP Ports” in the document “HiPath Gateways HG 3500 and HG 3575”. |
| Routing | The default host route, which is configured for HG 3575 in the same shelf, is used for the access point. |
| Firewall | The central processor only allows connections to addresses that it knows, i.e. access points or assigned service PCs. |
| Number of connections | Up to 83 TCP/IP connections (one per allocated access point) |

An additional “CUSTOMER“ interface is required for remote access by HiPath 4000 Manager and for accessing the file server, which distributes HiPath 4000 central system software and data.

| | |
|-------------|--|
| PHY | 10/100 Base T - autosensing |
| MAC address | Permanently programmed on the board, ->sticker (lower of the two addresses) |

Information for network administrators

Redundant LAN Interface

| | |
|-----------------------|---|
| IP address | Can be configured in the Unix system of the processor |
| Routing | Configurable |
| Number of connections | TCP/IP connection to file server if required. Administration via HiPath 4000 Assistant |
| Security | The same as for Unix in the HiPath 4000 central system |

10.5 Redundant LAN Interface



Only possible if HG 3500 is configured without WAML function!

Feature requirement

For increased resilience, HG 3500 and HG 3575 boards should be connected with two LAN cables to different switches.

Feature functionality

- Board is starting up:
 - If both LAN cables are connected and the HG board is starting up, LAN port 1 will always be activated.
LAN port 2 will be on standby, only layer 1 is active (higher protocol layers are down).
If only one LAN port is connected when the board is starting up (LAN1 or LAN2), that port will be used.
- If the active LAN port is disconnected/disabled by peer or equipment (when both LAN ports are connected):
 - The boards activate the standby LAN port.
 - The “new” port sends a GRATUITOUS ARP with the same MAC and IP addresses as the “old” port (the second MAC address will only be used if also another feature is configured at the interface (WAML/PPP router)).
 - When the board switches ports, the payload will be lost for < 2 sec – all active connections will be saved and NOT disconnected.
 - The port switch will be logged via HiPath-F message in HISTA.
 - If the “old” port comes up again, no port switchback will be performed.

Restriction

If the board is configured with FUNCTION=WAML in the AMO BFDAT, LAN port 1 is unable to switch over to LAN port 2 in the event of a fault.

This is because the feature WAML2/WAML Replacement is used for signaling survivability. This prevents the STMI board used from even operating redundant LAN interfaces.

Notes

- The boards only have one IP and MAC address.
- Only one port is active at a time.
- When the board starts up with two connected ports, LAN1 will be activated.
- No port switchback will be performed.
- No configuration in HiPath / HG boards is necessary to activate the feature.
- After installation of redundant LAN feature it is recommended to verify the functionality. The test can be performed by unplug the active LAN cable for at least 5 seconds and observe the switchover.

The reason for the test is to verify the correct behaviour of HG3500 in interaction with redundant IT/LAN infrastructure (e.g. L2 Switches/Router).

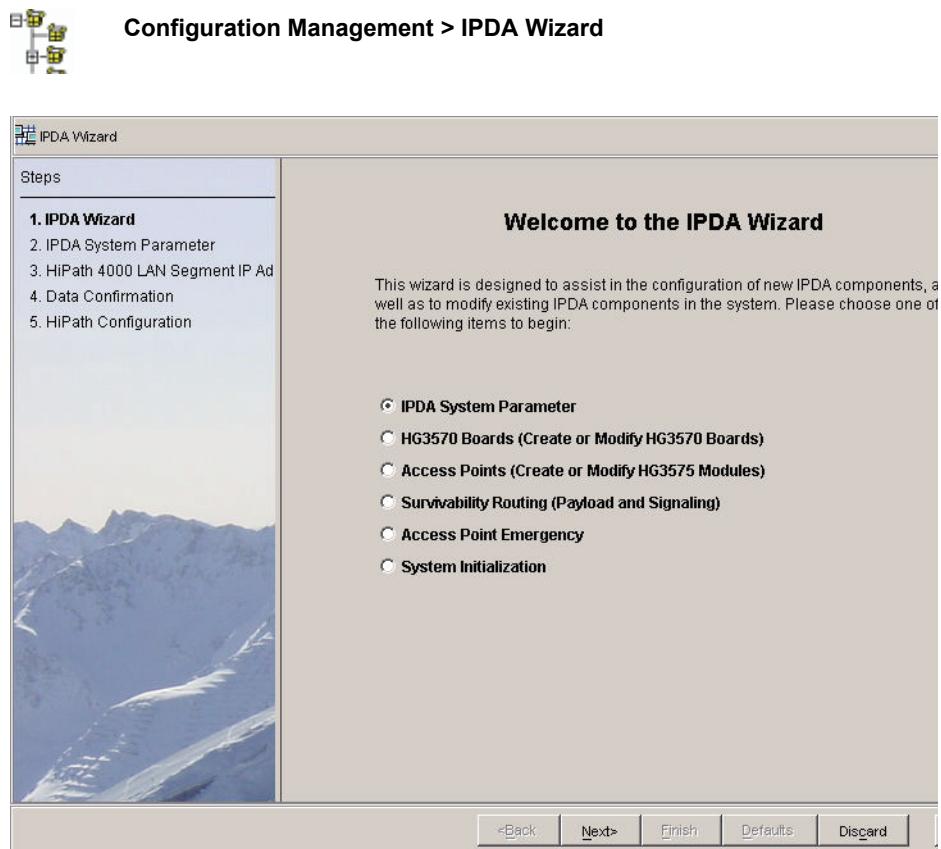
Information for network administrators

Redundant LAN Interface

11 IPDA Wizard

The IPDA Assistant provides a step-by-step user interface to help you with IPDA and HiPath 4000 SoftGate configuration.

You will find the assistant under:

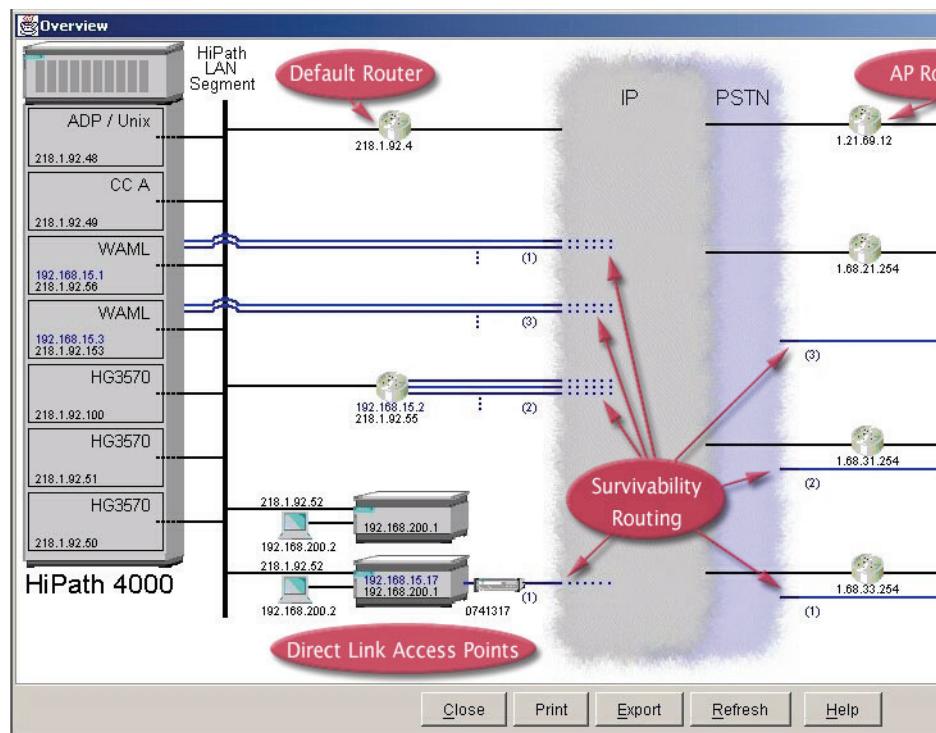


11.1 Functions

You can add or change the following IPDA components:

- **IPDA System Parameter**
- HG 3570 Boards (Create or Modify HG 3570 Boards)
- **Access Points (Create or Modify HG 3575 Modules)**
- **Survivability Routing (Payload and Signaling)**
- **Access Point Emergency**
- **System Initialization**

Additionally the assistant provides a graphical overview of the current IPDA configuration (button **Overview**):



IPDA System Parameter

The following functions are available:

- Configure System IP Addresses

IP addresses of the HiPath LAN segment, central processors, and the default router of the HiPath LAN segment.

- Configure Network Parameters

Parameters used for transmission bitrate, VLAN tagging and quality of service parameters are configured here.

- Configure Payload Quality Thresholds

Configure thresholds (e.g. timers) used to monitor transmission quality on a connection.

Access Points (Create or Modify HG 3575 Modules)

With this function you can configure new access points/HiPath 4000 SoftGates or modify existing access points/HiPath 4000 SoftGates. It is also possible to configure a new access point/HiPath 4000 SoftGate by using an already existing access point/HiPath 4000 SoftGate as template.

Result Access Point:

- AMO batch
- CLI batch (for configuring the NCUI board in the AP)

Result HiPath 4000 SoftGate:

- AMO batch
- xml file (for configuring the HiPath 4000 SoftGate)

Survivability Routing (Payload and Signaling)

Here you can configure alternate routes for the Signaling and payload connections to be used in case the IP network fails.

Access Point Emergency

With Access Point Emergency, additional control processors at access points (CC-AP) are deployed, which can take over control of a group of access points when these access points have lost connection to the host control processors (CC-A, CC-B) due to network failure or failure of the host system itself.

The following functions are available:

- Configure a local CC for an access point
- Configure a control processor located in an access point, which will be used in emergency situations.
- Configure an emergency group

Configure emergency group specific data, i.e. criteria for switching to emergency mode resp. back and the control processor to be used.

- Assign an access point to an emergency group

Here you can assign an individual access point to the emergency groups defined before or change the influence of this AP for switching the group to emergency mode.

- Configure alternate routing for emergency

Configure an alternate CO route per source group, which will be used in emergency situations.

System Initialization

You can perform the following under System Initialization

- Reset of Boards
Reload of HG3570 boards and/or access points.
- Loadware and SIU Files onto Access Points
Load new loadware onto access points.

- System Restarts

Execute Soft- or System-Restart on the HiPath4000 Switch.

- Switch Systemmode

Switch a system unit to emergency or normal mode.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

12 Short description how to install an AP Emergency (IPDA)

In the following part of the documentation, you were shown 2 examples of IPDA-configurations and its generating with AMO. Survivability, values of Tuning, QoS ... are not recommended in the generating. The standard values are used.

Example 1 shows a **Direct Link**-configuration (see [Section 12.1, "Example 1: "Direct Link" Access Point Emergency \(AP 17\) with own CO-Access and a second Access Point \(AP 18\)"](#)).

Example 2 shows a **Networked Link**-configuration (see [Section 12.2, "Example 2: "Networked Link" Access Point Emergency \(AP 17\) with an own CO-Connection and a second Access Point \(AP 18\)"](#)).

Direct Link

Direct Link means, that the AP-IP and the HiPath 4000 are in the **same** net segment.

Networked Link

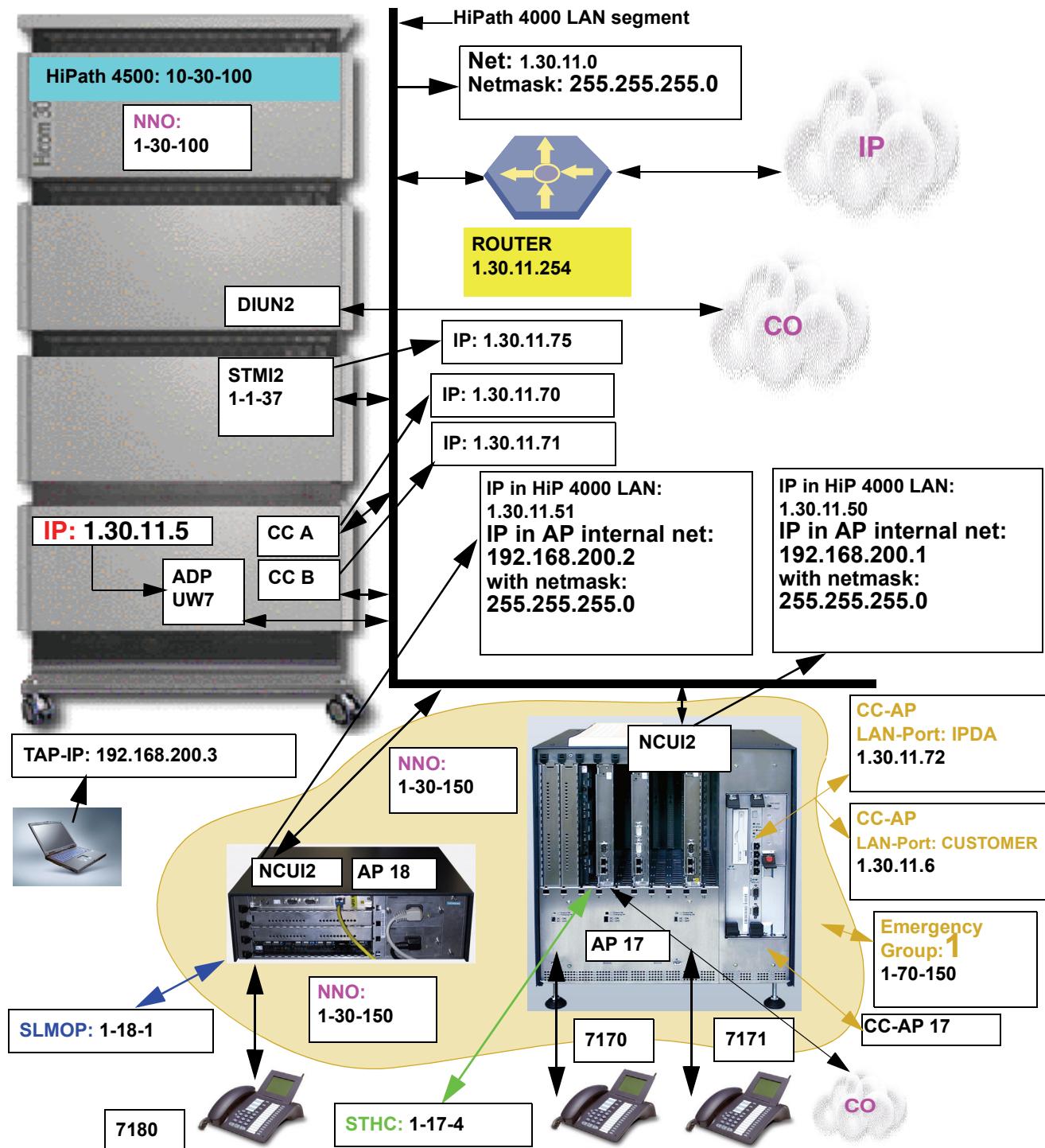
Networked Link means, that the AP-IP and the HiPath 4000 are in **different** net segments.

12.1 Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP 18)

The following example of generating is conformed to this configuration and IP situation:

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

12.1.1 Steps of installation in the HiPath 4000

Define the Net

```
ADD-
SIPCO:NETADDR=1.30.11.0,NETMASK=255.255.255.0,DEFRT=1.30.11.254,
CCAADDR=1.30.11.70,CCBADDR=1.30.11.71,SURVNET=0.0.0.0;
```

NOTE: A SURVNET in AMO SIPCO is to be generated, if the sales unit **Signaling Survivability** was bought, also if the feature isn't used (0.0.0.0). To use the feature AP Emergency, licences (**AP EMERGENCY**) have to be bought by the customer.

Survivability must be bought to use it

```
DISPLAY-CODEW;
SALES UNIT COUNTERS
=====
CODEWORD:
AFTKSB3CJYN4LKZN7GNWZH8TXH63M29A5GA2L2JN261LGKEA8CPHLZV5UGKHVPHP

XGRZDWDF83BG6BLE2U6LSP8GYS8VY5NADW88BUAE6RA58HXMD2N99TJSC9
VERSION : H205
SERIAL NUMBER: 7
HARDWARE ID : C6EB8F3B
ENTRY DATE : 22.02.2004
TRIAL MODE : NOT ACTIVATED
CONFIRMATION : 3706
```

| UNIT | CON- | USED | FREE | BLOCKED |
|--------------------------------|-------|------|------|---------|
| | TRACT | | | |
| COMSCENDO | 976 | 913 | 63 | |
| CORDLESS E | 0 | 0 | 0 | |
| PNE | 0 | 0 | 0 | |
| HIPATH PROCENTER ENTRY AGENT | 0 | 0 | 0 | |
| SIGNALING SURVIVABILITY | 10 | 0 | 10 | |
| CC-AP FOR AP EMERGENCY | 10 | 0 | 10 | |

Execute a BP-Soft-Restart

Normaly it's only neccessary using Change and Delete-operations.

```
EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=SOFT;
```

Install and configure the STMI2 Board

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=37,PARTNO="Q2316-X",
FCTID=1,LWVAR="0",IPADDR=1.30.11.75;

DISPLAY-BCSU:TYPE=TBL,LTG=1,LTU=1,SLOT=37;

ADDRESS : LTG 1 LTU 1 SOURCE GROUP 1
```

| ASSIGNED | MODULE | FCT | HWY | INSERTED | | | MODULE | |
|----------|--------|------|-----|----------|--------|-------|---------|--------|
| PEN | MODULE | TYPE | ID | BDL | MODULE | STATE | HW-INFO | STATUS |

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

```
--+-----+-----+-----+-----+-----+-----+-----+
 37 | Q2316-X      STM12      1 A | Q2316-X      | 1 | -D1 - | READY   |
 +-----+-----+-----+-----+-----+-----+-----+
 | IP ADDRESS : 1. 30. 11. 75 B-CHANNELS : 60 BCHLCNT : 60 |
 +-----+-----+-----+-----+-----+-----+
```

Generate the AP 17 and AP 18 with SRCGRP=17

ADD-UCSU:UNIT=AP,LTG=1,LTU=**17**,LTPARTNO="Q2305-X35 ",SRCGRP=17,
FRMTYPE=AP37009,**CONNTYPE=APDL**,LSRTADDR=1.30.11.50,APRTADDR=1.30.
11.254,
LOCID=001,LOCATION="BERLIN TI 1";

ADD-UCSU:UNIT=AP,LTG=1,LTU=**18**,LTPARTNO="Q2305-X35 ",SRCGRP=17,
FRMTYPE=INCH19,**CONNTYPE=APDL**,LSRTADDR=1.30.11.51,APRTADDR=1.30.1
1.254,
LOCID=002,LOCATION="BERLIN TI 2";

Configure the AP 17 and 18 in HiPath 4000 with TAP-IP-address

ADD-
APRT:TYPE=APNET,LTU=**17**,APIPADDR=192.168.200.1,NETMASK=255.255.255.0,
TAIPADDR=192.168.200.3;
ADD-
APRT:TYPE=APNET,LTU=**18**,APIPADDR=192.168.200.2,NETMASK=255.255.255.0,
TAIPADDR=192.168.200.3;

Activate LTU=17 and LTU=18

EXEC-USSU:MODE=CONFAP,LTU=17;
EXEC-USSU:MODE=CONFAP,LTU=18;

Generate the STHC Board in AP 17

ADD-BCSU : MTYPE=PER, LTG=1, LTU=17, SLOT=4, PARTNO="Q2169-X", FCTID=1;

Generate the SLMOP Board in AP 18

ADD-BCS: MTYPE=PER, LTG=1, LTU=18, SLOT=1, PARTNO="Q2169-X100", FCTID=1;

Generate a new Virtual Node (AP) and mark it as the DEFAULT-Node

ADD-KNDEF :NNO=1-30-
150,TYPE=OWN,ISDNCC=49,ISDNAC=30,ISDNLC=30150,ISDNSK=5,
ISDNUL=EXT;

CHANGE-KNDEF:NNO=1-30-150,DFLT=Y;

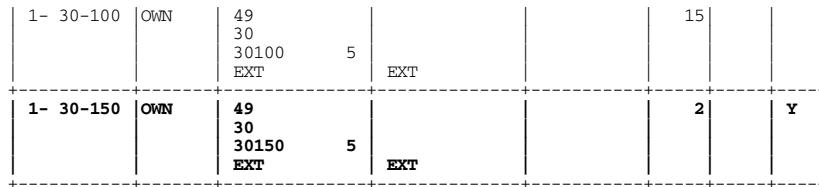
From now on, all stations, which are new generated, get the **Node number (NNO) = 1-30-150** automatically.

DISPLAY-KNDEF;

| Virtual Node Table | | | | | | | | | | |
|---------------------------|------|--------------|----|---------------|----|---------|----|-----------------|-----------------|-------|
| Virtual Node Number | Type | ISDN (E.164) | | Private (PNP) | | Unknown | | Popula- tion | CAC Pre- fix | Dflct |
| | | CC | | L2 | | | | | | |
| | | AC | | L1 | | | | | | |
| | | LC | SK | L0 | SK | NodeCD | SK | | | |
| | | UL | | UL | | | | | | |

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Generating of the three Stations in the Access Point (STHC and SLMOP Board)

```
ADD-SBCSU:STNO=7170,OPT=OPTI,CONN=DIR,PEN=1-17-4-
0,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,
COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP=0,STD=101,SECR=N,INS=Y,ALARMNO=
9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSSTNB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX
=5,HEADSET=N,HSKEY=NORMAL,CBKNAMB=Y,TEXTSEL=ENGLISH,HMUSIC=0,CAL
LOG=TRIES,COMGRP=0;
```

```
ADD-SBCSU:STNO=7171,OPT=OPTI,CONN=DIR,PEN=1-17-4-
1,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP
=0,STD=101,SECR=N,INS=Y,ALARMNO=9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSST
NB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAM
B=Y,TEXTSEL=ENGLISH,HMUSIC=0,CALLOG=TRIES,COMGRP=0;
```

```
ADD-SBCSU:STNO=7180,OPT=OPTI,CONN=DIR,PEN=1-18-1-
0,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP
=0,STD=101,SECR=N,INS=Y,ALARMNO=9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSST
NB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAM
B=Y,TEXTSEL=ENGLISH,HMUSIC=0,CALLOG=TRIES,COMGRP=0;
```

DISPLAY-SDAT:STNO=7170&&7171;

```
----- SUBSCRIBERDATA -----
STNO = 7170 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-17- 4- 0 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTISET LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
LCOSD1 = 5 SPDC1 = RCBKNA = NO
KEYSYS : NO LCOSD2 = 1 SPDC2 = 1

----- CDRACC =
SRCGRP = (17) CLASSMRK = EC G711 G729OPT
PUBNUM = TON =
NNO = 1 -30 -150 HOTIDX =
----- ATTRIBUTES -----
```

```
----- SUBSCRIBERDATA -----
STNO = 7171 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-17- 4- 1 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTIP500 LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
LCOSD1 = 5 SPDC1 = RCBKNA = NO
KEYSYS : NO LCOSD2 = 1 SPDC2 = 1

----- CDRACC =
SRCGRP = (17) CLASSMRK = EC G711 G729OPT
PUBNUM = TON =
NNO = 1 -30 -150 HOTIDX =
----- ATTRIBUTES -----
```

DISPLAY-SDAT:STNO=7180;

```
----- SUBSCRIBERDATA -----
STNO = 7180 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-18- 1- 0 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTISET LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
LCOSD1 = 5 SPDC1 = RCBKNA = NO
```

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

```
KEYSYS : NO          LCOSD2 = 1      SPDC2 = 1
-----
CDRACC =
SRCGRP = (17)           CLASSMRK = EC      G711     G729OPT
PUBNUM =
NNO   = 1 -30 -150        TON      =           NPI =
                                      HOTIDX =           ATTRIBUTES -----
```

```
CHANGE-KNDEF:NNO=1-30-100,DFLT=Y;
```

Set IP address and bit rate of the CC-AP (DSCXL) (LAN-Port: IPDA)

Prerequisite: ADD-DIMSU:TYPE=SYSTEM,CCAP=xx

```
ADD-
APESU:DATA=CCAP,CCAPNO=17,IPADDR=1.30.11.72,BITRATE="100MBFD";
```

NOTE: The CC-AP number must be one of the AP (LTU) numbers, which are configured in the system (normally the AP number, in which the CC-AP is installed) !!!

Add AP Emergency group

Prerequisite: ADD-DIMSU:TYPE=SYSTEM,APEGRP=xx

```
ADD-
APESU:DATA=APEGRP,EGRPNO=1,CCAPNO=17,THRSHLD=100,SBMODE=AUTO,NAM
E="TI-BLN",STABLE=5,SBBEGIN=20,SBEND=6,SBOFFSET=15;
```

The following settings are done there:

- a) Which CC-AP controls the Emergency group (CCAPNO).
- b) Name of the group (NAME).
- c) Switch back mode: manually or automaticly (SBMODE)
(using manual switch back the time interval is not relevant)
- d) Time interval
SBBEGIN (Begin (hour) for an automatical switch back)
SBEND (End (hour) for an automatical switch back)
SBOFFSET (Minutes for SBBEGIN and SBEND)
- e) Stable time for the LAN connection in minutes (STABLE).
- f) Threshold for the weighting alogrithm (THRSHLD). When reached or exceeded, the Access Points of the Emergency Group are switched over into control of the CC-AP.

Add AP 17 and AP 18 for AP-Emergency

```
ADD-APESU:DATA=AP,APNO=17,EGRPNO=1,WEIGHT=100,SWMODE=GROUP;
```

```
ADD-APESU:DATA=AP,APNO=18,EGRPNO=1,WEIGHT=100,SWMODE=GROUP;
```

Add the display text, which should be shown at the optiset/optiPoint in case of Emergency mode

```
CHANGE-ZANDE:TYPE=ALLDATA,APEDTXT="EMERGENCY";
```

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

Define the switch over delay

e.g.: if a RELOAD of the host should not activate the Emergency mode, a switch over delay can be set (in minutes).

```
DISPLAY-SIPCO:TYPE=TIMING;
```

```
H500: AMO SIPCO STARTED
```

```
TIMING :
```

```
-----  
PINGTIME ( TIME FOR CHECK PAYLOAD PATH QUALITY ) : 60 SEC  
RESTIME ( SELFRESET TIME AFTER SIG. CONN. LOSS ) : 60 SEC  
SUPVTIME ( KEEP ALIVE TIME SUPERVISORY ) : 4 SEC  
APESWDLY ( APE SWITCH OVER DELAY TIME. ) : 0 MIN  
ALVTIME ( KEEP ALIVE TIME SIGNALLING ) : 60 SEC
```

```
CHANGE-SIPCO:TYPE=TIMING,APESWDLY=8;
```

Display the AP Emergency configuration

```
DISPLAY-APESU:;
```

```
+-----+  
| CURRENT SYSTEM TIME : 09-17-2004 09:40:27 |  
+-----+  
+-----+  
| CC-AP: 17 IP ADDRESS: 1 .30 .11 .72  
| SPEED/WORKING MODE(IPDA): 100MBFD |  
+-----+  
+-----+  
| AP EMERGENCY GROUP: 1 CC-AP: 17 NAME: TI MUC  
| THRSHLD: 100 SEMODE: AUTO |  
| STABLE: 5 MIN SBBEGIN: 20 H SBEND: 6 H SBOFFSET: 15 MIN |  
+-----+  
| AP: 17 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP  
| CONTROL-UNIT: UNKNOWN SIGNAL-PATH: NONE |  
| LAST RECORDED CONNECTION STATUS CHANGE:  
|  
| HOST-CC: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00  
| CC-AP: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00 |  
+-----+  
| AP: 18 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP  
| CONTROL-UNIT: UNKNOWN SIGNAL-PATH: NONE |  
| LAST RECORDED CONNECTION STATUS CHANGE:  
|  
| HOST-CC: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00  
| CC-AP: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00 |  
+-----+
```

Activate the adaptive Jitterbuffer for the STM and NCUI board

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=JB,JBMODE=2;
```

```
CHANGE-STMIB:MTYPE=NCUII2,LTU=17,TYPE=JB,JBMODE=2;
```

```
CHANGE-STMIB:MTYPE=NCUII2,LTU=18,TYPE=JB,JBMODE=2;
```

LCR for the AP with own CO-Connection

- Define Target-group (AMO: **BUEND**)
- Generate trunk (trunks) (AMO: **TDCSU**)
- Define route (LRTG) (AMO: **RICHT**)
- Possibly define outdialing rule(s) (AMO: **LDR**)
- Generate LCR-route (AMO: **LDAT**)

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

- Define **Source depending routing**, that means a call, which is evaluated by the same Dialing plan (LDPLN), is routed to different LOUTEs depending on the Source-Group of the calling party.
Stations of the HiPath 4000 (NNO=1-30-100) are routed to that LROUTE, which has resulted in the allocation of the own CO-trunk (DIUNx-board). Therefor new stations of the AP (NNO=1-30-150) could be routed for the same dialing information to that LROUTE, which has resulted in the allocation of the own CO-trunk (STHC-board).
The controlling of this routing is realized by the AMO: **LPROF**.
- Generate the Dialing Plan (AMO: **LDPLN**). Don't use the parameter **LROUTE**, but the parameter **PROFIDX (profile index)**, which was generated by AMO LPROF.

Update of the BP-Database

`EXEC-UPDAT:UNIT=BP, SUSY=ALL;`

Time Synchronization for the Central System

An exact time is required for many HiPath 4000 functions. Up until now there was only one clock per system, but with AP Emergency there are up to 84 clocks in the system and they have to operate synchronously. Time is synchronized via the Unix system. It is configured using the Unix Basic Administration system.

There are two options:

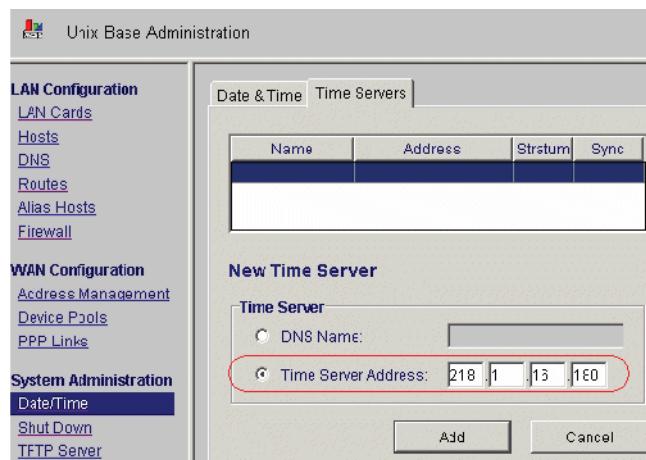
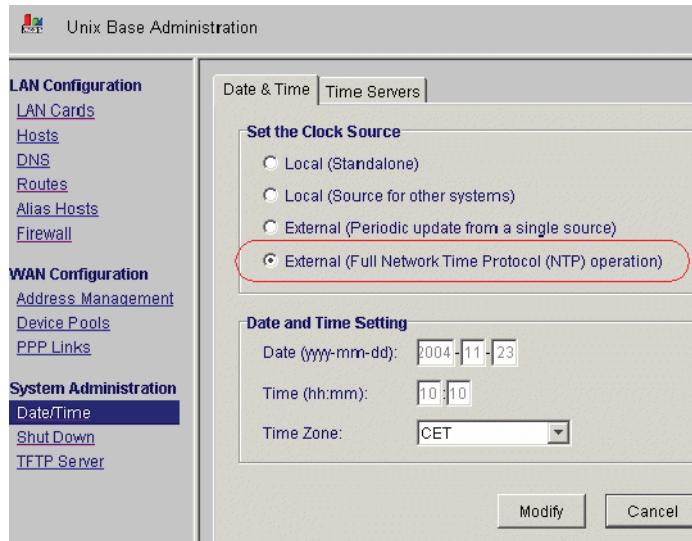
1. A time server is available in the IP network, which supports time synchronization of all HiPath 4000 processors (ADP and all CC-APs) using the network time protocol.
2. A time server is **not** available in the IP network. The HiPath 4000 central system must make its time available to all CC-APs via the network for synchronization purposes.

refers to 1: Time server in the IP Network

Menü: **Basis Administration > Unix Basis Administration > Date/Time**

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

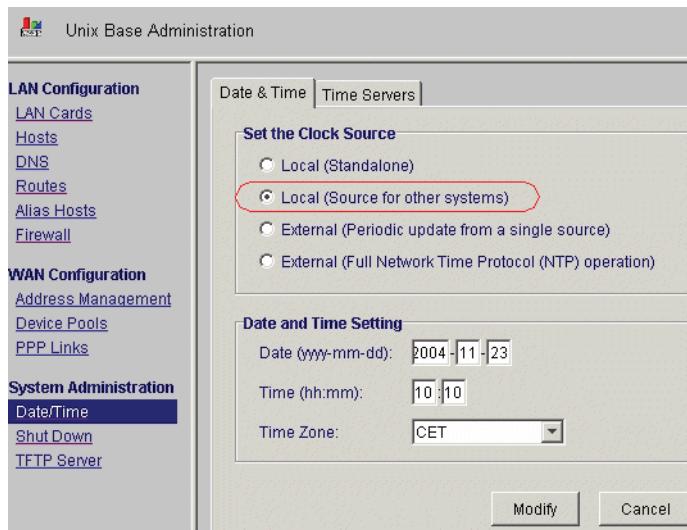


refers to 2: HiPath 4000 central system as time server

Menü: **Basis Administration > Unix Basis Administration > Date/Time**

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Configuring the AP Backup Server in the Host

HiPath 4000 Assistant:

Menu: **Software Management > Backup & Restore > AP Backup-Server**

NOTE: You can use as Login **rsta** or **apeftp**.

The login **apeftp** takes care of a secure transfer of the password.

Using **rsta** as filetransfer login the password will be transferred in clear.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

Host

Protocol: NFS FTP
[10] Maximal number of concurrent CC-AP transfers

IP Address: [1] [30] [11] [5] Login: [rsta]
(Don't use IP Address together with Host Name)
(For security reasons use apettp as login. For details see Service Documentation, section Complex Solutions, Configuring the APE Feature.)

Host Name: [] Password: [*****]
Directory: [/AS/BACKUP/IPDA] Account: []

Additional Information:

Refresh Test Configure

NOTE: In this example the HiPath 4000 Host is the AP Backup-Server itself. The directory ".AS/BACKUP/IPDA" is prepared in Unix.

Configuring of a schedule for the Backup

Menu: Software Management > Backup & Restore > Schedule

Step 1: Add new (entry)

Step 2: Start now

[Home Page](#)

[Backup](#) [Restore](#) [Content](#) [Status](#) [History](#) [Schedule](#) [GLA/PDS](#) [Administration](#) [MO/Tape](#) [Backup Server](#) [AP Backup Server](#)

| Type | Unit | Status | Frequency | Time | Archive | S | V |
|--------------|------|---------|-----------|-------|------------------|---|---|
| No entries | | | | | | | |
| AP Emergency | All | Enabled | Daily | 22 00 | AP Backup Server | Y | N |

S - Synchronize data before backup (Yes/No)
V - Verify data after write (Yes/No)

Copyright © 2004 Siemens AG. All rights reserved. HiPath 4000 Backup&Restore Version 0.122

Refresh Start now Add New

NOTE: By fixing the schedule for the Backup, the time for transferring the data to the CC-APs is defined indirectly. Maximum 10 minutes (not possible to control) after the Backup, the CC-APs find out, that a newer Backup-Set is available and get the Delta automatically!

After the first installation the first Backup must be started manually (Step 2), to be able to install the feature completely.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

After the manual Backup:

The screenshot shows the 'Backup' tab selected in the left sidebar. The main area displays a table of backup operations:

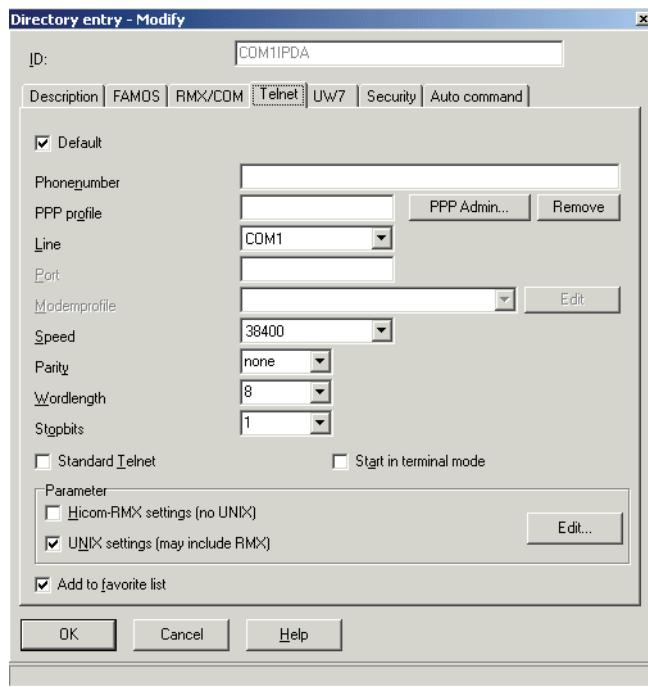
| Operation | Date/Time | Type | Archive | Unit | Status | Mode | Additional Information |
|-----------|------------------|--------------|------------------|------|------------|------|------------------------|
| Backup | 2004-09-17 10:14 | AP Emergency | AP Backup Server | RMX | Successful | Man | logfile |
| Backup | 2004-09-17 10:14 | AP Emergency | AP Backup Server | UNIX | Successful | Man | logfile |
| Backup | 2004-09-17 10:24 | AP Emergency | AP Backup Server | Save | Successful | Man | |

Buttons at the bottom right include 'Refresh' and 'Cancel backup'. The footer notes 'Copyright © 2004 Siemens AG. All rights reserved.' and 'HiPath 4000 Backup&Restore Version 0.12'.

12.1.2 Steps to configure the Access Points 17 and 18

Configure the NCUI2 Board in the Access Points

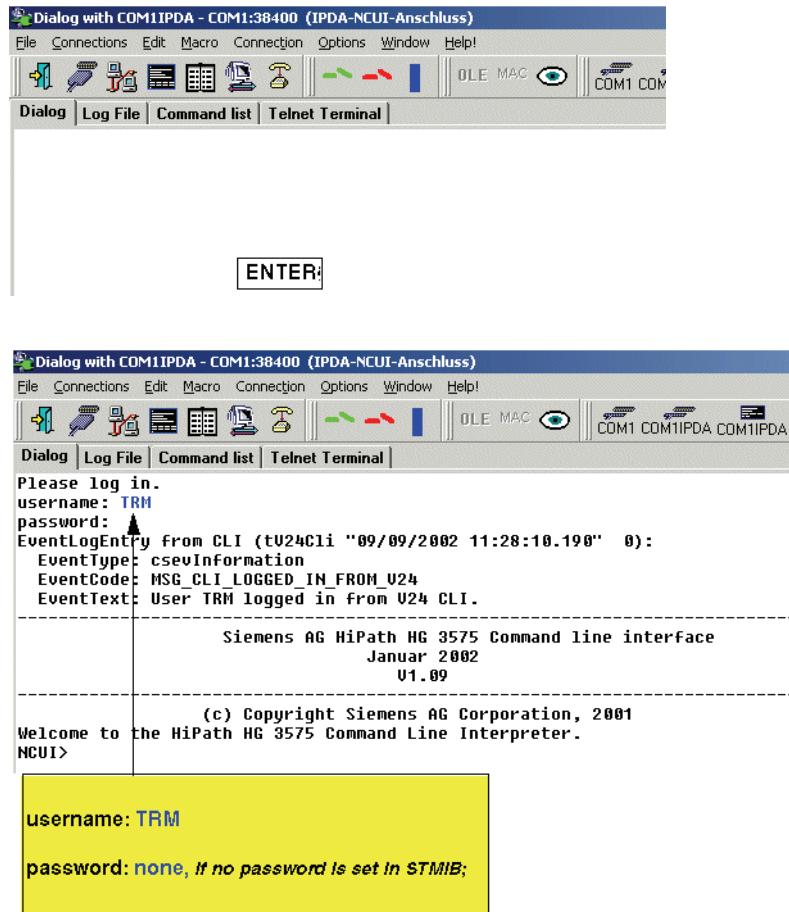
- Connect COM1 to the Service Interface of the NCUI2 in AP 17 (crossed cable)
- Start a TELNET-Session via a COM-connection (ComWin)



- LOGON under the Dialog - Tab.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

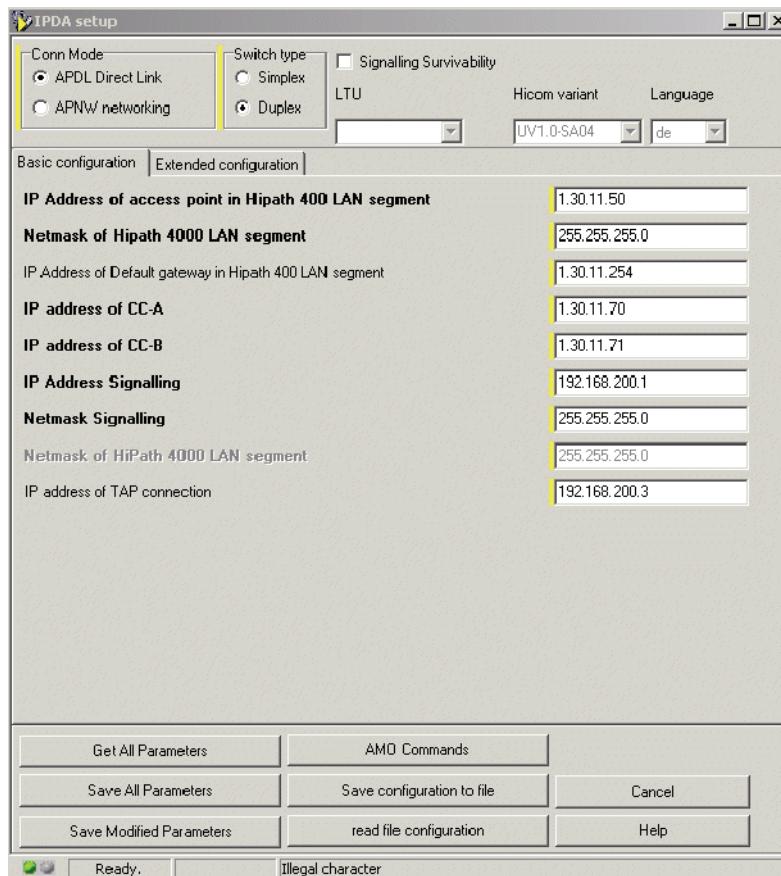


- Macro > Start CBL/Macro Bookmark > NCUI-Konfiguration or
Macro > Start CBL > Change to directory Apps > start NCUI.cbl.

Fill in all necessary settings in tab **Basic configuration** for the **AP 17**.

Short description how to install an AP Emergency (IPDA)

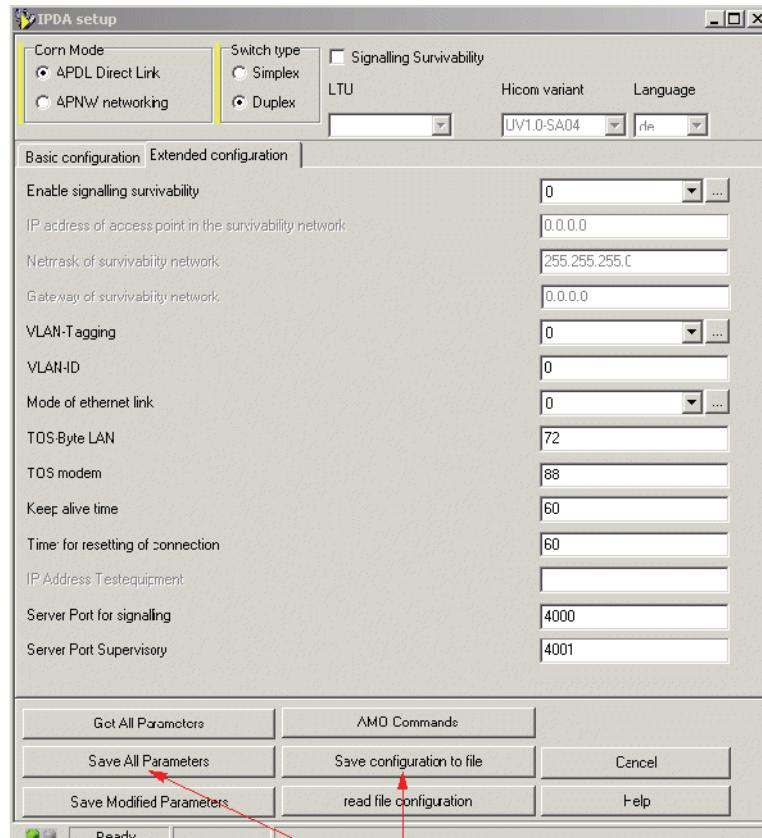
Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Change to the tab **Extended configuration**.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



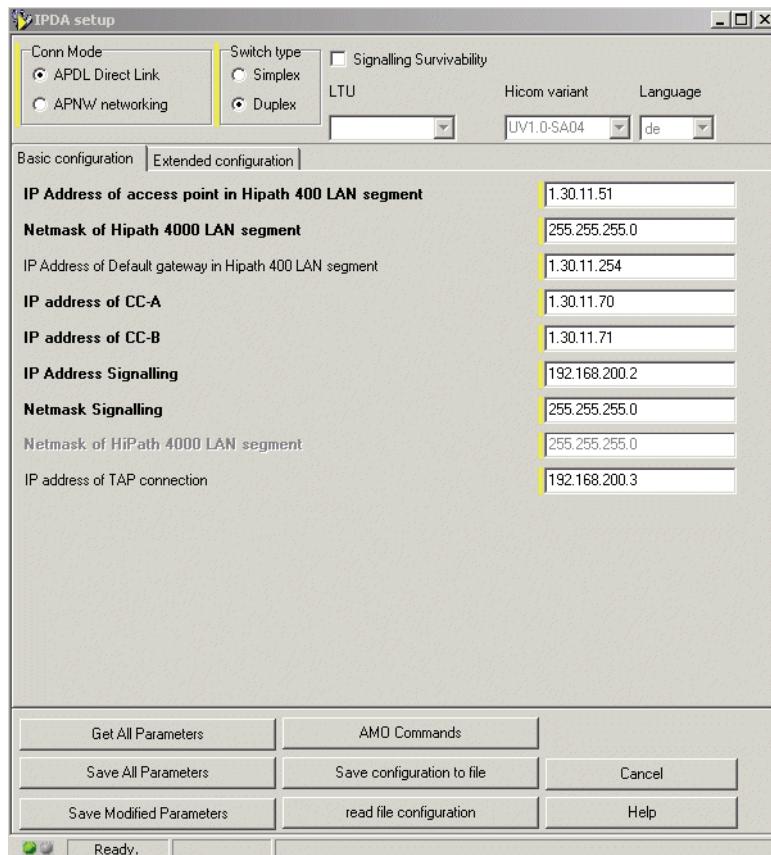
It's possible to save all settings to a file. Start the save-job (sending the new parameters to the AP).

- Connect the PC to the Service interface of AP 18 and logon (see AP 17)
**Macro > Start CBL/Macro Bookmark > NCUI-Konfiguration or
Macro > Start CBL > Change to directory Apps > start NCUI.cbl.**

Fill in all necessary settings in tab **Basic configuration** for the **AP 18**.

Short description how to install an AP Emergency (IPDA)

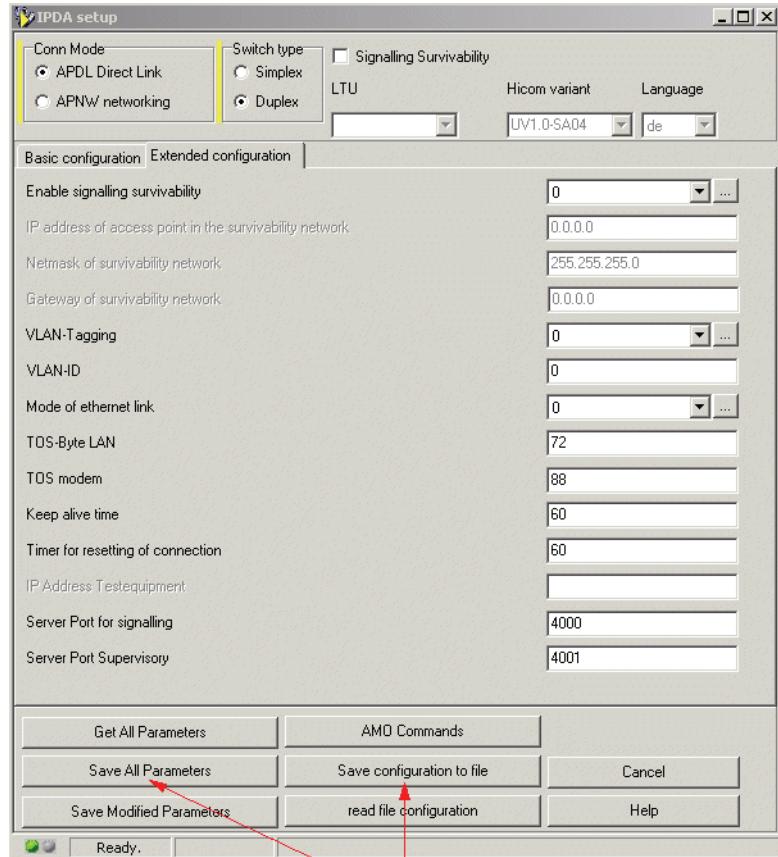
Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Change to the tab **Extended configuration**.

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



It's possible to save all settings to a file. Start the save-job (sending the new parameters to the AP).

Useful commands in the Telnet-connection for the NCUI2 board :

- show all parameters
- reboot
- ping

Reset AP 17 and 18

The APs could be reloaded either with the command "reboot" in the Telnet-session or push the **RESET-BUTTON** on the NCUI2 board.

Display the Status of the APs

```
DISPLAY-BCSU:TYPE=TBL,LTU=17;
```

| ADDRESS : LTG 1 LTU 17 SOURCE GROUP 17 | | | | | | | |
|--|-----------------|-------------|----------------|-----------------|-------|---------|---------------|
| PEN | ASSIGNED MODULE | MODULE TYPE | FCT/HWY ID BDL | INSERTED MODULE | STATE | HW-INFO | MODULE STATUS |
| 1 | AVAILABLE | | | AVAILABLE | | | |
| 2 | AVAILABLE | | | AVAILABLE | | | |
| 3 | AVAILABLE | | | AVAILABLE | | | |

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

| | | | | | | | |
|---|----------------------------|-------|-----------|-----------|--------------|-------|-------|
| 4 | Q2169-X | STHC | 1 A | Q2169-X | 1 | -G2 - | READY |
| 5 | AVAILABLE | | | AVAILABLE | | | |
| 6 | Q2302-X10 | NCUI2 | 1 | Q2305-X35 | 1 | -07 - | READY |
| +-----+-----+-----+-----+-----+-----+-----+-----+ | | | | | | | |
| | IP ADDRESS : 1. 30. 11. 50 | | BCHL : 60 | | BCHLCNT : 60 | | |
| 7 | AVAILABLE | | | AVAILABLE | | | |
| 8 | AVAILABLE | | | AVAILABLE | | | |
| 9 | AVAILABLE | | | AVAILABLE | | | |
| 10 | AVAILABLE | | | AVAILABLE | | | |

DISPLAY-BCSU:TYPE=TBL,LTU=18;

ADDRESS : LTG 1 **LTU 18** SOURCE GROUP 17

| PEN | ASSIGNED MODULE | MODULE TYPE | FCT ID | HWY BDL | INSERTED MODULE | STATE | HW-INFO | MODULE STATUS |
|-----|----------------------------|----------------|-----------|------------|--------------------|-------|---------|------------------|
| 1 | Q2169-X100 | SLMOP | 1 | A | Q2169-X100 | 1 | -07 - | READY |
| 2 | AVAILABLE | | | | AVAILABLE | | | |
| 3 | AVAILABLE | | | | AVAILABLE | | | |
| 4 | Q2302-X10 | NCUI | 1 | | Q2302-X10 | 1 | -07 - | READY |
| | IP ADDRESS : 1. 30. 11. 51 | | BCHL : 60 | | BCHLCNT : 60 | | | |
| 5 | AVAILABLE | | | | AVAILABLE | | | |
| 6 | AVAILABLE | | | | AVAILABLE | | | |
| 7 | AVAILABLE | | | | AVAILABLE | | | |
| 8 | AVAILABLE | | | | AVAILABLE | | | |

Send the actual data to the APs (for security)

EXEC-USSU:MODE=UPDATAP,LTU=17,LOADTYPE=UL;

EXEC-USSU:MODE=UPDATAP,LTU=18,LOADTYPE=UL;

Preparing the HD of the CC-AP and executing the RMX configuration

NOTE: Don't connect the CC-AP to the Customer LAN at this time !

That means no LAN cable is connected to the "CUSTOMER" and to the "IPDA" Port of the DSCXL board.

1. Prepare a MOD with the **same** APS version, which is running in the Host (HiPath 4000).
2. Boot the CC-AP using this MOD.
3. Connect the Service-PC (TAP) to the DSCXL of the CC-AP, using the LAN-Port "SERVICE" of the DSCXL board. Set the LAN interface of the Service-PC e.g. to the IP address 192.0.2.100. Start the HiPath Expert Access.
4. Copy the APS to the HD of the CC-AP:

```
DEACTIVATE-DSSM:UNIT=A1,CNO=1;
START-INIT:UNIT=A1,DEVNAME=A1H11;
COPY-DDRSM:UNIT=A1,MASTERID=6,MASTERAR=E&I,SLAVEID=1,
SLAVEAR=E&I;
```

NOTE: An additional possibility is to boot the CC-AP with any MOD (ADP Ready) and to transfer the corresponding software with the tool PCHI.

5. Reload the CC-AP -> Unix fist installation is executed (90 minutes);

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

6. Execute the RMX-configuration of the CC-AP:

```
EXEC-DBC:ARCH=4000, ARCHTYPE=1;  
EXEC-APC;  
CHANGE-  
DATE:YEAR=xxxx,MONTH=xx,DAY=xx,HOUR=xx,MINUTE=xx,SECOND=xx;  
CHANGE-CPCI :TYPE=SYSCONF,MONO=YES,RTM=NO,OEM=NO;  
EXEC-UPDAT:UNIT=A1,SUSY=ALL;  
EXEC-REST:TYPE=SYSTEM,RSLEVEL=RELOAD;  
  
ADD-APESM:APNO=17;  
EXEC-UPDAT:UNIT=A1,SUSY=ALL;  
EXEC-REST:TYPE=SYSTEM,RSLEVEL=RELOAD;
```

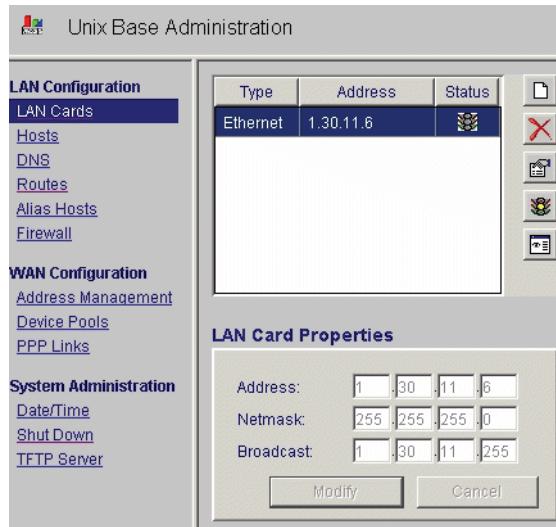
Configuration of Unix for the CC-AP

Start the Internet Explorer and connect with the IP "http://192.0.2.5".

User name: rsta
Password: Siemens2000

Configure LAN card (LAN-Port: CUSTOMER on the DSCXL board)

Menu: **Basis Administration > UNIX Basis Administration > LAN Card**

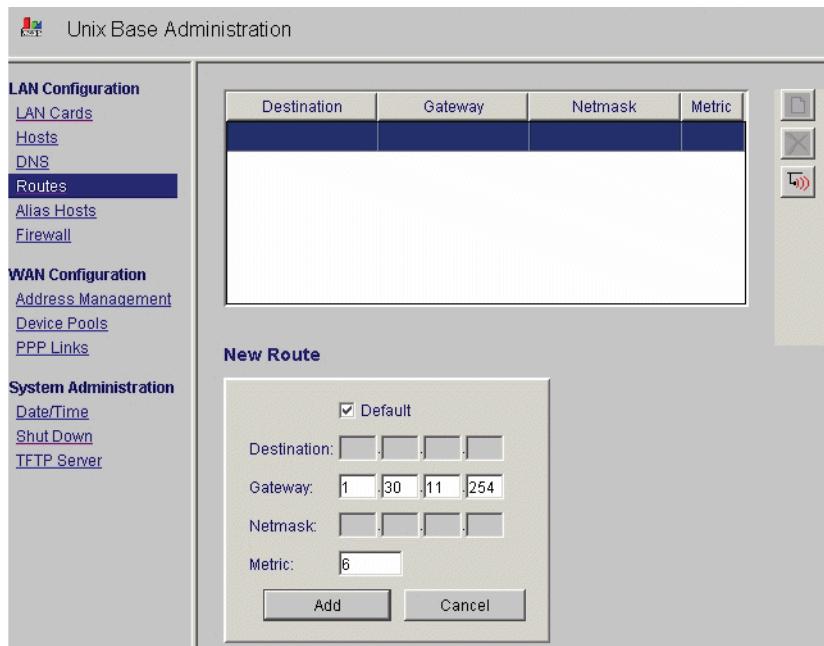


Add the Default Router (not necessary by all means for a "Direct Link" configuration)

Menu: **Basis Administration > UNIX Basis Administration > Routes**

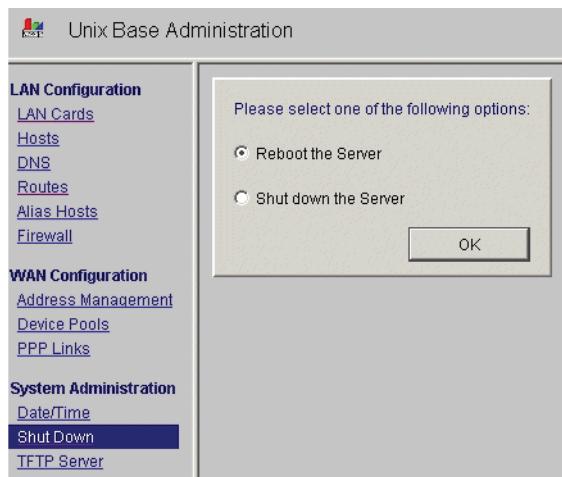
Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Reboot the UNIX-Server

Menu: Basis Administration > UNIX Basis Administration > Shut Down



Connections to the Customer LAN

NOTE: Now the two customer LAN cable must be plugged to the "CUSTOMER-Port" and the "IPDA-Port" of the CC-AP DSCXL board !

Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

Configuration of the time synchronization in the CC-AP

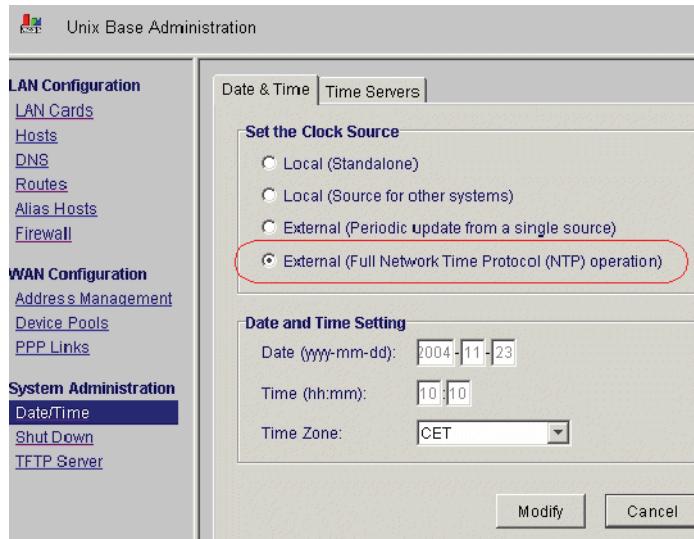
The time of the CC-AP must run in synch with the clock in the central system. Time is synchronized via the Unix system. It is configured using the Unix Basic Administration system.

There are two options:

1. A time server is available in the IP network, which supports time synchronization of all HiPath 4000 processors (ADP and all CC-APs) using the network time protocol.
2. A time server is **not** available in the IP network. The HiPath 4000 central system makes its time available to all CC-APs via the network for synchronization purposes.

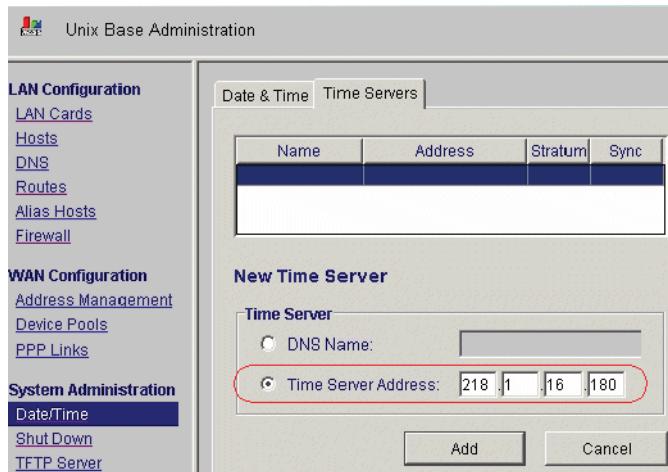
refers to 1: NTP server in the IP Network

Menü: **Basis Administration > Unix Basis Administration > Date/Time**



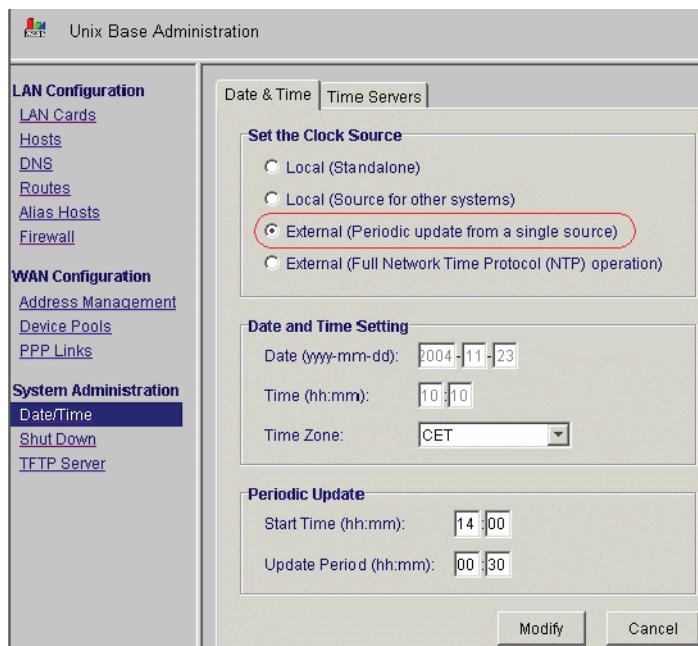
Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



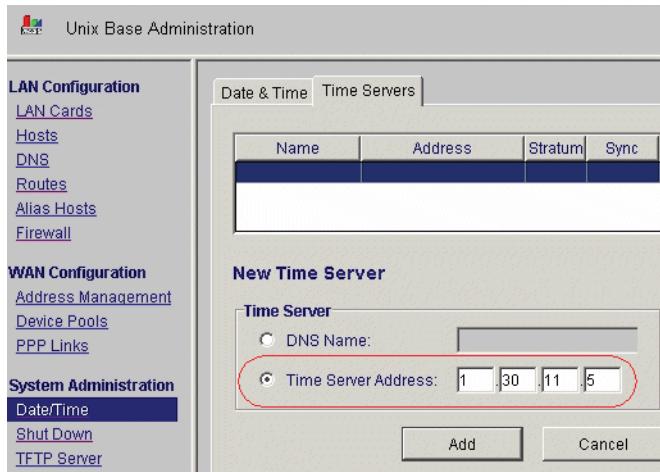
refers to 2: HiPath 4000 Central System as Time Server

Menü: Basis Administration > Unix Basis Administration > Date/Time



Short description how to install an AP Emergency (IPDA)

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP



Configuring the AP Backup Server in the CC-AP

NOTE: Make sure, that the Backup in the Host has finished **successfully!!**

HiPath 4000 Assistant:

Menu: **Software Management -> Backup & Restore -> AP Backup-Server**

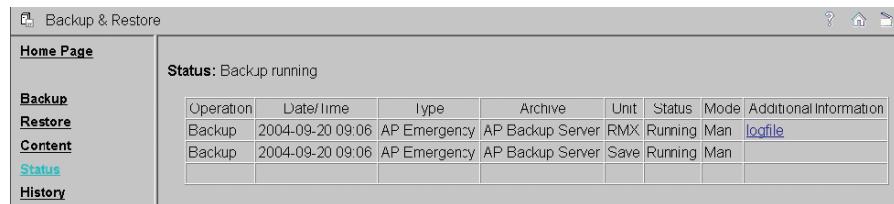
NOTE: You can use as **Login rsta or apeftp**. The login **apeftp** takes care of a secure transfer of the password. Using **rsta** as filetransfer login the password will be transferred in clear.

The screenshot shows the 'Backup & Restore' interface of the HiPath 4000 Assistant. The left sidebar lists various options like Home Page, Backup, Restore, Content, Status, History, Schedule, GLAPDS, Administration, MO/Tape, Backup Server, AP Backup Server (which is selected), and Log Files. The main panel is titled 'Administration Backup AP Server' and shows configuration for an AP server named 'CC-AP (17)'. It includes fields for Protocol (NFS or FTP, with FTP selected), IP Address (1.30.11.5), Login (rsta), Host Name, Directory (/AS/BACKUP/IPDA), Password, and Account. A note at the bottom states: '(For security reasons use apeftp as login. For details see Service Documentation, section Complex Solutions, Configuring the APE Feature.)'. At the bottom are Refresh, Test, and Configure buttons.

Short description how to install an AP Emergency (IPDA)

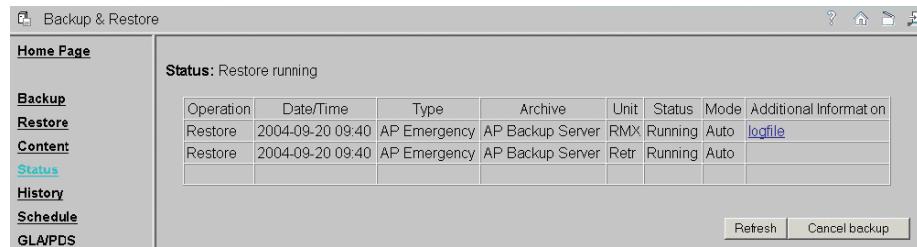
Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

After this step the access to the AP Backup-Server is generated. In the menu **Backup & Restore > Status** you can now watch to the actions of the CC-AP. During the First Installation the CC-AP will first start a Backup to have a predefined start situation.



The HiPath Backup & Restore application running in the CC-AP will now check all 10 minutes, if there is a new complete Backup set in the AP Backup-Server (in this case the Host), will download the delta data and will activate it.

The time for the Restore process depends on the amount of data and the available transfer band width between AP Backup-Server and the CC-AP. The process needs at least 30 minutes.



Display the APE status

DISPLAY-APESU;

```
+-----+
| CURRENT SYSTEM TIME : 09-20-2004 10:40:30 |
+-----+
+-----+
| CC-AP: 17 IP ADDRESS: 1 .30 .11 .72
| SPEED/WORKING MODE(IPDA): 100MBFD |
+-----+
+-----+
| AP EMERGENCY GROUP: 1 CC-AP: 17 NAME: TI MUC
| THRSHLD: 100 SBMODE: AUTO
| STABLE: 5 MIN SBBEGIN: 20 H SBENDE: 6 H SBOFFSET: 15 MIN |
+-----+
| AP: 17 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP
| CONTROL-UNIT: HOST-CC SIGNAL-PATH: LAN
| LAST RECORDED CONNECTION STATUS CHANGE:
|   HOST-CC: CONNECTED: YES CONNECTED SINCE : 2004-09-20 10:37
|   CC-AP: CONNECTED: YES CONNECTED SINCE : 2004-09-20 10:37 |
+-----+
| AP: 18 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP
| CONTROL-UNIT: HOST-CC SIGNAL-PATH: LAN
| LAST RECORDED CONNECTION STATUS CHANGE:
|   HOST-CC: CONNECTED: YES CONNECTED SINCE : 2004-09-20 10:38
|   CC-AP: CONNECTED: YES CONNECTED SINCE : 2004-09-20 10:38 |
+-----+
```

Example 1: "Direct Link" Access Point Emergency (AP 17) with own CO-Access and a second Access Point (AP

12.1.3 Verification and Acceptance of the AP Emergency Configuration

It is essential that the function of the AP Emergency configuration be verified by an acceptance test after the initial startup and after substantial modifications.

To this end, each emergency group must be switched over once to the CC-AP for administration. In emergency operation, it must then be verified that communication to the trunk, to other systems in the network, and among emergency groups at different CC-APs functions as planned. Where applicable, also include installed applications that support emergency operation in the test.

Also verify the communications capability of access points that can be switched to the CC-AP independently of the emergency group when the group is running in normal operation.

You can conduct the tests when the system load is low.

The following Administartor Switchovers can be used:

- all access points of all emergency groups of all CC-APs in the system
EXEC-APESU : SYSMODE=EMERG , LEVEL=SYST ; (switches to the CC-AP)
EXEC-APESU : SYSMODE=NORMAL , LEVEL=SYST ; (switches to the central control)
- all access points of all emergency groups of one CC-AP
EXEC-APESU : SYSMODE=EMERG , LEVEL=CCAP , NO=99 ; (switches to the CC-AP)
EXEC-APESU : SYSMODE=NORMAL , LEVEL=CCAP , NO=99 ; (switches to the central control)
- all access points of one emergency group (of one CC-AP)
EXEC-APESU : SYSMODE=EMERG , LEVEL=APEGRP , NO=2 ; (switches to the CC-AP)
EXEC-APESU : SYSMODE=NORMAL , LEVEL=APEGRP , NO=2 ; (switches to the central control)
- one access point (of one emergency group (of one CC-AP))
EXEC-APESU : SYSMODE=EMERG , LEVEL=AP , NO=99 ; (switches to CC-AP)
EXEC-APESU : SYSMODE=NORMAL , LEVEL=AP , NO=99 ; (switches to the central control)

Short description how to install an AP Emergency (IPDA)

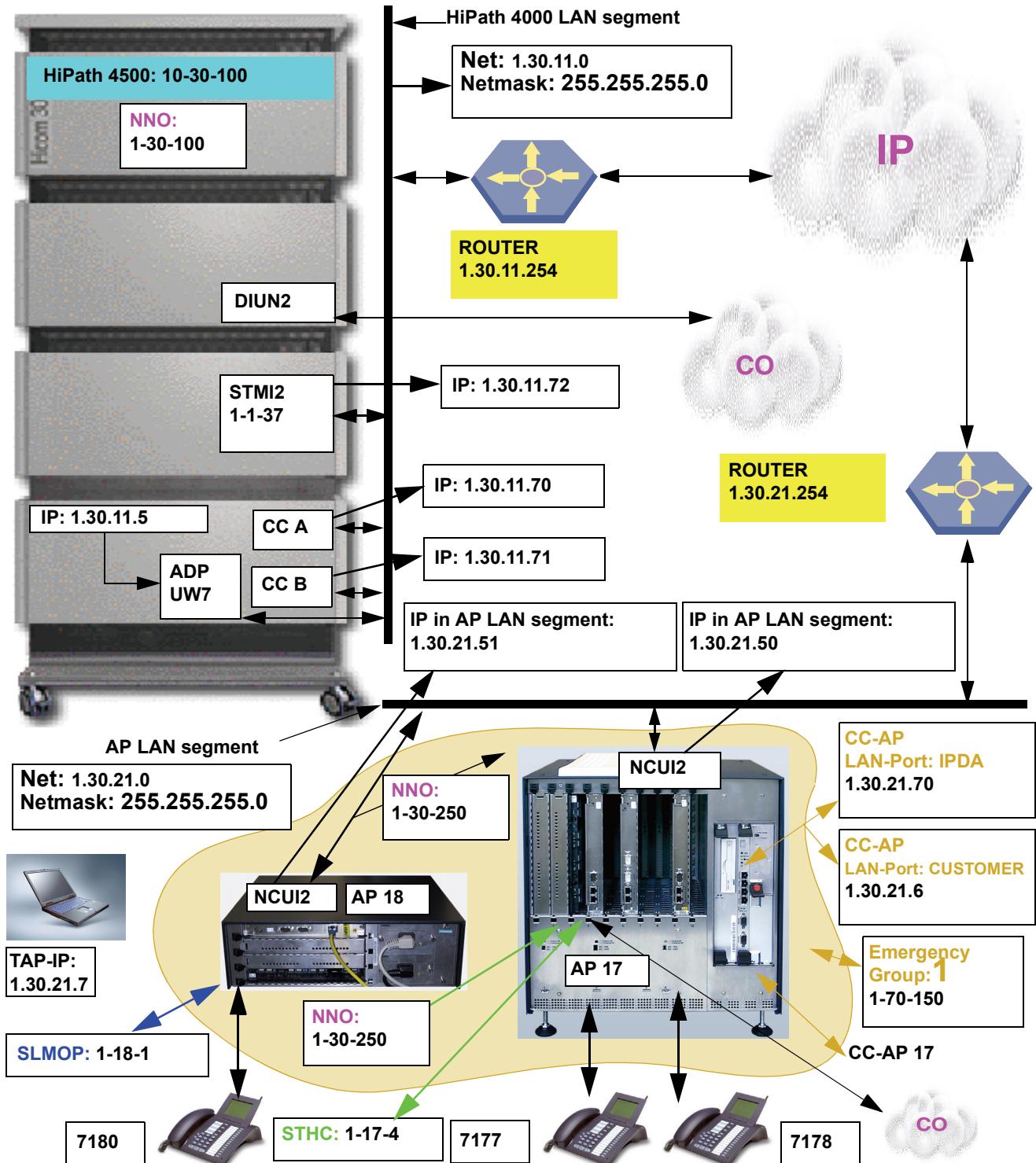
Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

12.2 Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access Point (AP 18)

The following example of generating is conformed to this configuration and IP situation:

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access



Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

12.2.1 Configuration steps in the HiPath 4000 V2.0

Define the Net

ADD-

```
SIPCO:NETADR=1.30.11.0,NETMASK=255.255.255.0,DEFRT=1.30.11.254,C  
CAADDR=1.30.11.70,CCBADR=1.30.11.71,SURVNET=0.0.0.0;
```

NOTE: A SURVNET in AMO SIPCO is to be generated, if the sales unit **Signaling Survivability** was bought, also if the feature isn't used (0.0.0.0). To use the feature AP Emergency, licences (**AP EMERGENCY**) have to be bought by the customer.

Survivability and CC-AP must be bought to use it

DISPLAY-CODEW;

SALES UNIT COUNTERS

=====

CODEWORD:

```
AFTKSB3CJYN4LKZN7GNWZH8TXH63M29A5GA2L2JN261LGKEA8CPHLZV5UGKHVPHP
```

```
XGRZDWDF83BG6BLE2U6LSP8GYS8VY5NADW88BUAE6RA58HXMD2N99TJSC9
```

VERSION : H205

SERIAL NUMBER: 7

HARDWARE ID : C6EB8F3B

ENTRY DATE : 22.02.2004

TRIAL MODE : NOT ACTIVATED

CONFIRMATION : 3706

| UNIT | CON-TRACT | USED | FREE | BLOCKED |
|--------------------------------|-----------|------|------|---------|
| COMSCENDO | 976 | 913 | 63 | |
| CORDLESS E | 0 | 0 | 0 | |
| PNE | 0 | 0 | 0 | |
| HIPATH PROCENTER ENTRY AGENT | 0 | 0 | 0 | |
| SIGNALING SURVIVABILITY | 10 | 0 | 10 | |
| CC-AP FOR AP EMERGENCY | 10 | 0 | 10 | |

Execute a BP-Soft-Restart

Normaly it's only neccessary using Change and Delete-operations.

EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=SOFT;

Install and configure STM12 board

ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=37,PARTNO="Q2316-X",FCTID=1, IPADDR=1.30.11.72;

DISPLAY-BCSU:TYPE=TBL,LTG=1,LTU=1,SLOT=37;

| ADDRESS : LTG 1 LTU 1 SOURCE GROUP 1 | | | | | | | |
|--------------------------------------|-----------------|-------------|--------|---------|-----------------|-------|-----------------------|
| PEN | ASSIGNED MODULE | MODULE TYPE | FCT ID | HWY BDL | INSERTED MODULE | STATE | HW-INFO MODULE STATUS |
| 37 | Q2316-X | STM12 | 1 | A | Q2316-X | 1 | -D2 - READY |

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

```
+-----+-----+-----+-----+
| IP ADDRESS : 1. 30. 11. 72      BCHL : 60      BCFLCNT : 60      |
+-----+-----+-----+-----+
```

Generate the AP 17 and AP 18 with SRCGRP=17

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2305-X35",SRCGRP=17,FRMTYPE=AP37009,CONNTYPE=APNW,LSRTADDR=1.30.11.254,APRTADDR=1.30.21.254,LOCID=001,LOCATION="MUNICH 1";
```

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=18,LTPARTNO="Q2305-X35",SRCGRP=17,FRMTYPE=INCH19,CONNTYPE=APNW,LSRTADDR=1.30.11.254,APRTADDR=1.30.21.254,LOCID=002,LOCATION="MUNICH 2";
```

Configure AP 17 and AP 18 in HiPath 4000 with TAP-IP address

```
ADD-APRT:TYPE=APNET,LTU=17,APIPADR=1.30.21.50,NETMASK=255.255.255.0,TAIPADR=1.30.21.7;
```

```
ADD-APRT:TYPE=APNET,LTU=18,APIPADR=1.30.21.51,NETMASK=255.255.255.0,TAIPADR=1.30.21.7;
```

Activate LTU=17 and LTU=18

```
EXEC-USSU:MODE=CONFAP,LTU=17;
```

```
EXEC-USSU:MODE=CONFAP,LTU=18;
```

Generate the STHC Board in AP 17

```
ADD-BCSU:MTYPE=PER,LTG=1,LTU=17,SLOT=4,PARTNO="Q2169-X",FCTID=1;
```

Generate the SLMOP Board in AP 18

```
ADD-BCSU:MTYPE=PER,LTG=1,LTU=18,SLOT=1,PARTNO="Q2169-X100",FCTID=1;
```

Generate a new Virtual Node (AP) and mark it as the DEFAULT node

```
ADD-KNDEF:NNO=1-30-  
250,TYPE=OWN,ISDNCC=49,ISDNAC=89,ISDNLC=722,ISDNSK=3,ISDNUL=NST;  
CHANGE-KNDEF:NNO=1-30-250,DFLT=Y;
```

From now on, all stations, which are new generated, get the **Node number (NNO) = 1-30-250** automatically.

```
DISPLAY-KNDEF;
```

| VIRTUAL NODE TABLE | | | | | | | | |
|---------------------------|------|--------------------------|----------------------|--------------------------|-----------------------|-----|------|--|
| VIRTUAL NODE NUMBER | TYPE | ISDN (E.164) | PRIVATE (PNP) | UNKNOWN | POPUP- LA- TION | CAC | DFLT | |
| 1- 30-100 | OWN | 49 30 30100 EXT | L2 L1 L0 UL | SK NODECD SK UL | | 15 | | |
| 1- 30-250 | OWN | 49 89 722 EXT | 3 | EXT | | 0 | Y | |

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

Generating of the three subscribers in Access Points

```
ADD-SBCSU:STNO=7177,OPT=OPTI,CONN=DIR,PEN=1-17-4-
0,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP
=0,STD=101,SECR=N,INS=Y,ALARMNO=9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSST
NB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAM
B=Y,TEXTSEL=ENGLISH,HMUSIC=0,CALLOG=ALL,COMGRP=0;
```

```
ADD-SBCSU:STNO=7178,OPT=OPTI,CONN=DIR,PEN=1-17-4-
1,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP
=0,STD=101,SECR=N,INS=Y,ALARMNO=9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSST
NB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAM
B=Y,TEXTSEL=ENGLISH,HMUSIC=0,CALLOG=ALL,COMGRP=0;
```

```
ADD-SBCSU:STNO=7180,OPT=OPTI,CONN=DIR,PEN=1-18-1-
0,DVCFIG=OPTISET,TSI=1,COS1=13,COS2=11,LCOSV1=5,LCOSV2=1,LCOSD1=
5,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=1,SPDI=0,SPDC2=1,IDCR=N,REP
=0,STD=101,SECR=N,INS=Y,ALARMNO=9,RCBKB=N,RCBKNA=N,DSSTNA=N,DSST
NB=Y,DIGNODIS=N,OPTIDA=1,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAM
B=Y,TEXTSEL=ENGLISH,HMUSIC=0,CALLOG=ALL,COMGRP=0;
```

```
DISPLAY-SDAT:STNO=7177&&7178;
```

```
-- SUBSCRIBERDATA --
STNO = 7177 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-17- 4- 0 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTISET LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
KEYSYS : NO LCOSD1 = 5 SPDC1 = RCBKNA = NO
          LCOSD2 = 1 SPDC2 = 1

CDRACC =
SRCGRP = (17) CLASSMRK = EC G711 G729OPT
PUBNUM =
NNO = 1 -30 -250 TON = NPI =
HOTIDX =

----- ATTRIBUTES -----
-- SUBSCRIBERDATA --
STNO = 7178 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-17- 4- 1 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTIP500 LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
KEYSYS : NO LCOSD1 = 5 SPDC1 = RCBKNA = NO
          LCOSD2 = 1 SPDC2 = 1

CDRACC =
SRCGRP = (17) CLASSMRK = EC G711 G729OPT
PUBNUM =
NNO = 1 -30 -250 TON = NPI =
HOTIDX =

----- ATTRIBUTES -----
```

```
DISPLAY-SDAT:STNO=7180;
```

```
-- SUBSCRIBERDATA --
STNO = 7180 COS1 = 13 DPLN = 0 SSTNO = NO
PEN : 1-18- 1- 0 COS2 = 11 ITR = 0 TRACE = NO
DVCFIG : OPTISET LCOSV1 = 5 COSX = 1 ALARMNO = 9
AMO : SBCSU LCOSV2 = 1 SPDI = 0 RCBKB = NO
KEYSYS : NO LCOSD1 = 5 SPDC1 = RCBKNA = NO
          LCOSD2 = 1 SPDC2 = 1

CDRACC =
SRCGRP = (17) CLASSMRK = EC G711 G729OPT
PUBNUM =
NNO = 1 -30 -250 TON = NPI =
HOTIDX =

----- ATTRIBUTES -----
```

```
CHANGE-KNDEF:NNO=1-30-100,DFLT=Y;
```

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

Set IP address and bit rate of the CC-AP (DSCXL) (LAN-Port: IPDA)

Prerequisite: ADD-DIMSU:TYPE=SYSTEM,CCAP=xx

ADD-
APESU:DATA=CCAP,CCAPNO=17,IPADDR=1.30.21.70,BITRATE="100MBFD";

NOTE: The CC-AP number must be one of the AP (LTU) numbers, the CC-AP is responsible for !!!

Add AP Emergency group

Prerequisite: ADD-DIMSU:TYPE=SYSTEM,APEGRP=xx

ADD-
APESU:DATA=APEGRP,EGRPNO=1,CCAPNO=17,THRSHLD=100,SBMODE=AUTO,
NAME="TI-BLN",STABLE=5,SBBEGIN=20,SBEND=6,SBOFFSET=15;

The following settings are done there:

- a) Which CC-AP controls the Emergency group (CCAPNO).
- b) Name of the group (NAME).
- c) Switch back mode: manually or automatically (SBMODE)
(using manual switch back the time interval is not relevant)
- d) Time interval
SBBEGIN (Begin (hour) for an automatical switch back)
SBEND (End (hour) for an automatical switch back)
SBOFFSET (Minutes for SBBEGIN and SBEND)
- e) Stable time for the LAN connection in minutes (STABLE).
- f) Threshold for the weighting algorithm (THRSHLD). When reached or exceeded, the Access Points of the Emergency Group are switched over into control of the CC-AP.

Add AP 17 and 18 for AP-Emergency

ADD-APESU:DATA=AP,APNO=17,EGRPNO=1,WEIGHT=100,SWMODE=GROUP;

ADD-APESU:DATA=AP,APNO=18,EGRPNO=1,WEIGHT=100,SWMODE=GROUP;

Add the display text, which should be shown at the optiset/optiPoint in case of Emergency mode

CHANGE-ZANDE:TYPE=ALLDATA,APEDTXT="EMERGENCY";

Define the switch over delay

e.g.: if a RELOAD of the host should not activate the Emergency mode, a switch over delay can be set (in minutes).

DISPLAY-SIPCO:TYPE=TIMING;

H500: AMO SIPCO STARTED

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

```
TIMING :  
-----  
PINGTIME ( TIME FOR CHECK PAYLOAD PATH QUALITY ) : 60 SEC  
RESTIME ( SELFRESET TIME AFTER SIG. CONN. LOSS ) : 60 SEC  
SUPVTIME ( KEEP ALIVE TIME SUPERVISORY ) : 4 SEC  
APESWDLY ( APE SWITCH OVER DELAY TIME. ) : 0 MIN  
ALVTIME ( KEEP ALIVE TIME SIGNALLING ) : 60 SEC
```

```
CHANGE-SIPCO:TYPE=TIMING,APESWDLY=8;
```

Display the AP Emergency configuration

```
DISPLAY-APESU:;
```

```
+-----+  
| CURRENT SYSTEM TIME : 09-17-2004 09:40:27 |  
+-----+  
+-----+  
| CC-AP: 17 IP ADDRESS: 1 .30 .21 .70  
SPEED/WORKING MODE(IPDA): 100MBFD |  
+-----+  
+-----+  
| AP EMERGENCY GROUP: 1 CC-AP: 17 NAME: TI MUC  
THRSHLD: 100 SEMODE: AUTO  
STABLE: 5 MIN SBBEGIN: 20 H SBENDE: 6 H SBOFFSET: 15 MIN |  
+-----+  
| AP: 17 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP  
CONTROL-UNIT: UNKNOWN SIGNAL-PATH: NONE  
LAST RECORDED CONNECTION STATUS CHANGE:  
HOST-CC: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00  
CC-AP: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00 |  
+-----+  
| AP: 18 AP EMERGENCY GROUP: 1 CC-AP: 17 WEIGHT: 100 SWMODE: GROUP  
CONTROL-UNIT: UNKNOWN SIGNAL-PATH: NONE  
LAST RECORDED CONNECTION STATUS CHANGE:  
HOST-CC: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00  
CC-AP: CONNECTED: NO DISCONNECTED SINCE : 0000-00-00 00:00 |  
+-----+
```

Activate the adaptive Jitterbuffer for the STMI and NCUI board

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=JB,JBMODE=2;
```

```
CHANGE-STMIB:MTYPE=NCUII2,LTU=17,TYPE=JB,JBMODE=2;
```

```
CHANGE-STMIB:MTYPE=NCUII2,LTU=18,TYPE=JB,JBMODE=2;
```

LCR for the AP 17 with own CO-Connection

- Define Target-group (AMO: **BUEND**)
- Generate trunk (trunks) (AMO: **TDCSU**)
- Define route (LRTG) (AMO: **RICHT**)
- Possibly define outdialing rule(s) (AMO: **LODR**)
- Generate LCR-route (AMO: **LDAT**)
- Define **Source depending routing**, that means a call, which is evaluate by the same
Dialing plan (LDPLN), is routed to different LOUTEs depending on the Source-Group of the calling party.
Stations of the HiPath 4000 (NNO=1-30-100) are routed to that LROUTE, which has result in the allocation of the own CO-trunk (DIUNx board).
Therefor new stations of the AP (NNO=1-30-250) could be routed for the same dialing information to that

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

LROUTE, which has result in the allocation of the own CO-trunk (STHC board).

The controlling of this routing is realized by the AMO: **LPROF**.

- Generate the Dialing Plan (AMO: **LDPLN**). Don't use the parameter **LROUTE**, but the parameter **PROFIDX (profile index)**, which was generated by AMO LPROF.

Update of the BP-Database

```
EXEC-UPDAT:MODUL=BP,SUSY=ALL;
```

Time Synchronization for the Central System

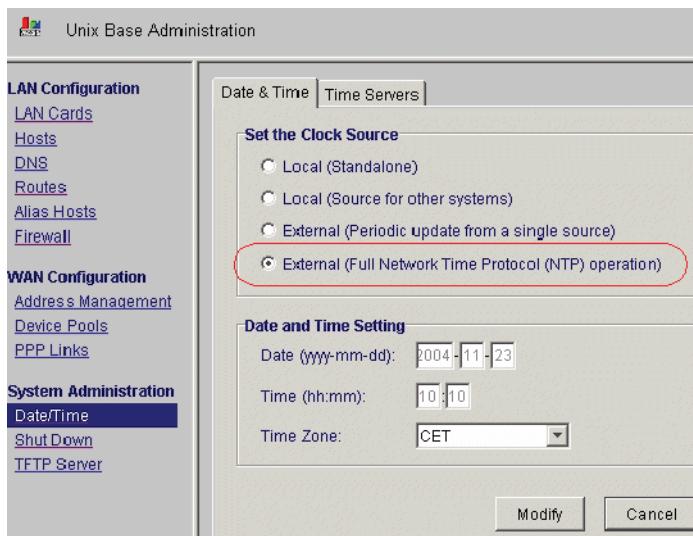
An exact time is required for many HiPath 4000 functions. Up until now there was only one clock per system, but with AP Emergency there are up to 84 clocks in the system and they have to operate synchronously. Time is synchronized via the Unix system. It is configured using the Unix Basic Administration system.

There are two options:

1. A time server is available in the IP network, which supports time synchronization of all HiPath 4000 processors (ADP and all CC-APs) using the network time protocol.
2. A time server is **not** available in the IP network. The HiPath 4000 central system must make its time available to all CC-APs via the network for synchronization purposes.

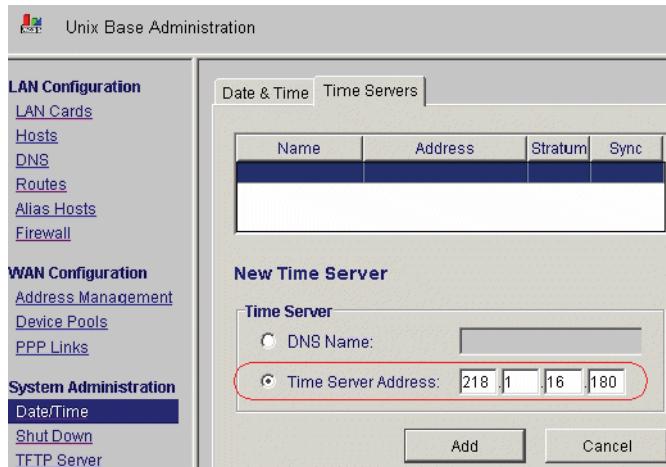
refers to 1: Time server in the IP Network

Menü: **Basis Administration > Unix Basis Administration > Date/Time**



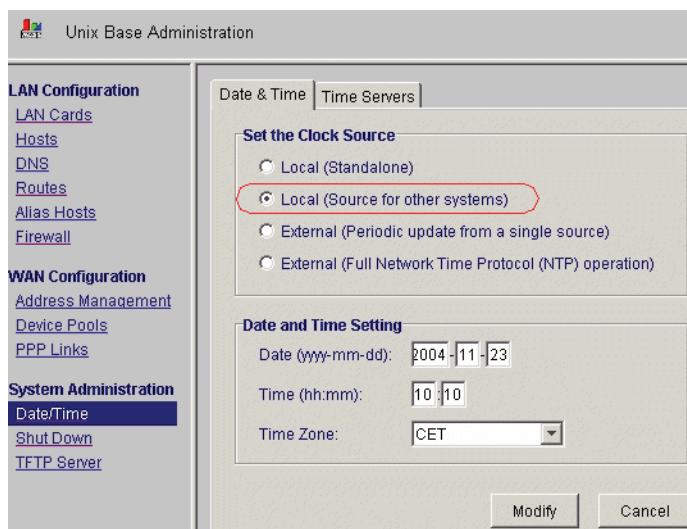
Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access



refers to 2: HiPath 4000 central system as time server

Menü: **Basis Administration > Unix Basis Administration > Date/Time**



Configuring the AP Backup Server in the Host

HiPath 4000 Assistant:

Menu: **Software Management > Backup & Restore > AP Backup-Server**

Short description how to install an AP Emergency (IPDA)

Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access

Host

Administration Backup AP Server

Protocol: NFS FTP
[10] Maximal number of concurrent CC-AP transfers

IP Address: [1] [30] [11] [5] Login: [rsta]

(Don't use IP Address together with Host Name)
(For security reasons use apeftp as login. For details see Service Documentation, section Complex Solutions, Configuring the APE Feature.)

Host Name: [] Password: [*****]
Directory: [/AS/BACKUP/IPDA] Account: []

Additional Information:
[]

Refresh Test Configure

NOTE: In this example the HiPath 4000 Host is the AP Backup-Server itself. The directory "/.AS/BACKUP/IPDA" is prepared in Unix.

Configuring of a schedule for the Backup

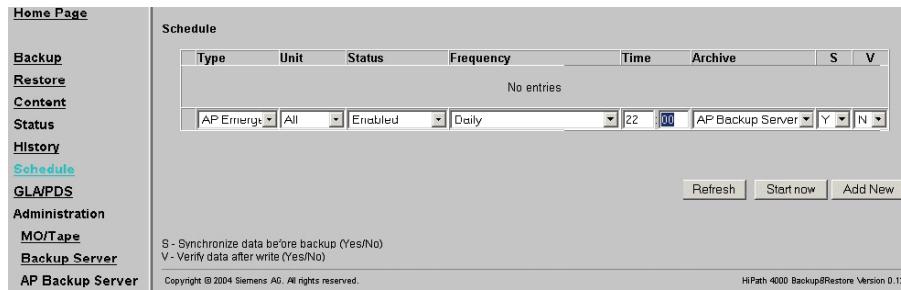
Menu: **Software Management > Backup & Restore > Schedule**

Step 1: Add New (entry)

Step 2: Start now

Short description how to install an AP Emergency (IPDA)

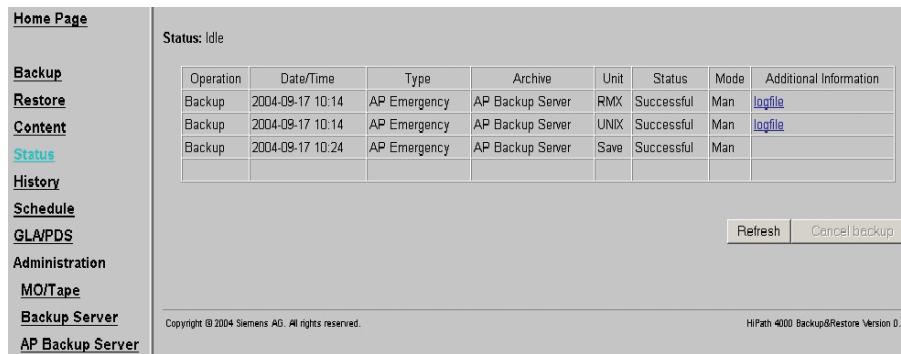
Example 2: "Networked Link" Access Point Emergency (AP 17) with an own CO-Connection and a second Access



NOTE: By fixing the schedule for the Backup, the time for transferring the data to the CC-APs is defined indirectly. Maximum 10 minutes (not possible to control) after the Backup, the CC-APs find out, that a newer Backup-Set is available and get the Delta automatically!

NOTE: After the first installation the first Backup must be started manually (Step 2), to be able to install the feature completely.

After the manual Backup:



13 FAQs - Frequently Asked Questions

1. **Question:** Do I actually need a HG 3500 board in the central system for every AP 3300 IP or AP 3500 IP access point?

Answer: NO, definitely not. It is always assumed that there must be a fixed relationship between a HG 3575 and a HG 3500 to transfer signaling data. However, signaling data comes directly from the central processor (via the SL 200 or SL 100 module). The HG 3500 is only responsible for payload transport.

The number of HG 3500s required in the system depends solely on the traffic volume between the access points (total for all APs) and the central system.

2. **Question:** How can I ensure that a HG 3500 crash does not automatically affect associated access points?

Answer: HG 3500s are not allocated to any specific access points. If there are several HG 3500s in the system, then they share the overall traffic volume. HG 3500 seizure is performed cyclically in the system, i.e. the first connection is routed via the first HG 3500, the next via the second and so on. If an HG 3500 fails, all active calls over this board are interrupted. The board is then no longer seized for new calls. These new calls are then routed via the other HG 3500s, as capacity allows.

3. **Question:** Why are IPDA components not allowed to be connected via hubs?

Answer: Hubs work in Ethernet's classic "shared medium" mode. All connected units share the total bandwidth. Jeder kann alles mithören. Nur einer kann zu einem Zeitpunkt senden.

Voice communication is bidirectional. The data flow from A to B is the same size (expect using VAD) as the dataflow from B to A. As transmission is only possible from one unit at a time in shared medium mode, the send and receive direction each occupy the same share of the total bandwidth available.

The use of layer 2 switches, which are nowadays often cheaper than hubs, decouples the connection media of the individual units. All units can simultaneously send and receive. The bandwidth (now available for each unit) can be used more efficiently.

4. **Question:** Why are the LAN ports on the IPDA components set by default to *Autonegotiate*? There are many reports that this can lead to problems.

Answer: The default setting should ensure that initial startup runs relatively smoothly. However, on account of the recurring problems encountered with autonegotiation, we strongly urge you to enter a **fixed** setting for **both** interface partners.

It is essential to configure both interfaces - with the same values - at the same time. When using an autonegotiate interface with one that is fixed, the autonegotiate interface often fails to "negotiate" to the fixed interface's setting. Please also refer to the Note on page 4-43.

5. **Question:** Is it necessary to enter the network address for the HiPath 4000 LAN segment in the AMO SIPCO? Does every HiPath 4000 need a separate LAN segment or can I operate multiple HiPath 4000 systems in the same LAN segment?

Answer: You can operate multiple HiPath 4000 systems in the same network. In this case, the components' IP addresses must not be used more than once and the capacity of the router or WAN connection must suffice for the entire bandwidth requirement.

6. **Question:** The effect of default setting recommended by popular router manufacturers and the TOS byte default values documented for IPDA, that is, the pre-defined DiffServ CodePoints (DSCP) is exactly the opposite of the intended effect. The packets we marked as high priority are rejected straightaway by the router. What is this nonsense about?

Answer: The default values used for IPDA come from an internal Siemens standard that was implemented in all HG 35xx gateways. The interoperability problem has since come to light with the result that the company standard will be modified shortly.

The default values can be modified at any time and modified in line with actual conditions in the customer network.

7. **Question:** Does IPDA support VLANs?

Answer: Yes but only in conjunction with priority tagging. In accordance with IEEE 802.1 p/q, tagging was introduced for IPDA to support priority tagging. If tagging is activated then the permanently preset priority bits of the various types of traffic are always set (see the last column of Table 2 "TOS values" in document "HiPath Gateways HG 3500 and HG 3575"). If tagging is active, the VLAN ID can also be set (default value is zero). VLAN ID is not supported without the set priority bits.

8. **Question:** Does IPDA support subnetting (RFC 950)?

Answer: Yes. When the network mask is entered, a check is performed to determine whether the block of ones that has been set meets the minimum length required for the class of the address, i.e. 8 ones for Class A, 16 for B and 24 for C. If the number of ones is greater than the number required for the class, subnetting is activated.

9. **Question:** Does IPDA support supernetting (RFC 1338)?

Answer: No.

10. **Question:** The failure tolerance of the HiPath 4000 central system with duplex processors is indeed very good. However, the SL200 interfaces of the processors are not duplicated. Does this mean that I immediately lose all access points in the event of the LAN connection of the active processor failing?

Answer: No, the redundancy concept of the HiPath 4000 covers the failure of the LAN connection to the HiPath 4000 LAN segment. Both processors, i.e. including the standby processor, constantly monitor the availability of the LAN connection to the HiPath 4000 LAN segment. If the connection of the active processor fails and the standby processor connection is OK, the processor is changed over immediately and the standby processor takes over operation.

11. **Question:** Can an access point be operated such that signaling is only routed via IP? Voice can be routed as a dial-up connection via ISDN as in the case of payload survivability.

Answer: Payload survivability is designed as an emergency solution in the event of an IP network crash/malfunction. Only basic call functionality can be guaranteed.

You must also take into consideration that signaling via IP must offer Quality of Service which is often not supported when using external narrowband WAN links together with data communication in existing installations.

Follow-up question: It cannot be that difficult for an ISDN PABX to route voice connections via a carrier network.

Answer: The systems are designed for it. However, in the case described above, the system must call itself via the CO and negotiate this as an internal call with the complete range of features - and this in itself is not an easy task.

12. **Question:** Why does the “direct link” access point need additional IP addresses?

It must be easier to route a call in the same LAN segment than in multiple LAN segments with routers.

Answer: The reason for the internal router and the additional address is due to signaling survivability. For signaling survivability, TCP layer packets which can no longer be transported via LAN must be delivered on another route, that is, the survivability path, before the supervision timer in the TCP expires. The IP destination addresses must remain the same for this, only the router involved can be switched.

In the case of a “networked” access point, the (default) LAN router is switched to the survivability router.

This LAN router is not available in the case of a “direct link” access point, as CC and AP are in the same LAN segment. You cannot switch from *no* router to a survivability router. Consequently, signaling survivability could not be offered for “direct link”. The only practical solution is to integrate the LAN router in the access point. Two IP addresses are therefore provided for a “direct link” access point: the router port IP address at the HiPath 4000 LAN segment and the signaling instance IP address in the AP “internal network”.

13. **Question:** Is it possible to operate the IPDA components in a network that does not support Quality of Service?

Answer: If the entire network is ideally dimensioned, if there is no packet loss and no significant packet propagation time during long-term measurements and if the network load (including the IPDA load) is moderate on all paths, then an IPDA system will also function in this network without QoS measures. Malfunctions will occur if these conditions are violated, for example, through load displacement or something similar. Constant, highly developed network monitoring is essential in this case to recognize bottlenecks developing in the network and to remove them immediately.

If narrowband WAN connections which are also used for data connections and have a high load are utilized in the network used for IPDA, then malfunctions are guaranteed in networks without a QoS functionality for prioritizing IPDA traffic.

14. **Question:** A remote access point is connected via WAN. Transmission capacity is only 800 Kbps. Major interferences occur during peak traffic and the access point sometimes performs restarts. The traffic from/to the access point is prioritized higher compared to parallel, active data traffic. Can the bandwidth seized by HiPath 4000 on the WAN link be limited to 800 Kbps?

Answer: The bit rate required by the access point can be limited by the Resource Manager. Table 6-8 "High-priority load of an AP as a function of the permissible B-channels" on page 6-247 provides an overview of the capacity required as a function of the number of connections simultaneously active. The basis for this assumption is calls using the G.711 codec. The signaling load was set to 64 Kbps. With a sample size of 30 ms (default), nine connections could be used simultaneously to remain under 800 Kbps (792).

Follow-up question: Table 6-7 "High-priority load of an AP as a function of codec and sample size" on page 6-246 shows me that I can transport significantly more B-channels with the available bandwidth if I use the G.729 codec.

Answer: The 800 Kbps available could theoretically transport over 30 B channels if the sample size were set to 40 ms in G.729.

However, please note that in this case, all the trunks in the entire system involved in calls must be configured to support G.729 (classmark G729OPT). This is the default setting. All trunks in the access point must also be configured with classmark G729 which necessitates the use of the G.729 codec. This also applies to the conference connection and music-on-hold.

However, we advise against configuring the conference unit with G.729 if you want to guarantee the best voice comprehension levels possible for conferences.

It should also be noted that the **melody** played back when music-on-hold is active is distorted by the voice compression.

In addition, please note that fax machines, modems and ISDN data terminals must not operate with G.729 compression. If these devices are active, 81 Kbps will be seized (30 ms - in this example - with G.711 and 40 ms with G.729) instead of the anticipated 21 Kbps.

In other words, the number of B channels in this example must not be set

to 30 even with the maximum possible use of G.729. The correct value is between 9 and 30. It depends on how many G.711 connections are still required.

If the number of B channels is set too high, **ALL** connections will be affected when the capacity of the WAN link is exceeded. The signaling connection can also be affected and can, depending on the level of interference, cause a switchover to signaling survivability or an access point restart.

- 15. Question:** I'd like to dispatch an access point over ISDN. Given that NCUI only provides a LAN connection, I'd like to use a router with an S_0 interface. This offers me a bandwidth of 128 Kbps, which is enough for 7 B channels. I estimate the signaling volume to be very low. Should I expect any problems?

Answer: Yes, you should stay well clear of this configuration. Although 7 B channels require only 114 Kbps with G.729 compression and a sample size of 60 ms, there is good reason for always keeping around 64 Kbps free for signaling. This leaves only around 64 Kbps for payload. That is not sufficient, even if only one call cannot be compressed (fax, modem, ISDN data). See also Question 14 on page 13-356.

- 16. Question:** I'd like to use a PCM30 router between an access point and HiPath 4000 LAN segment, thus with a maximum of 2 Mbps of bandwidth available.

However, because the customer wants to use dial-up lines through the public telephone network instead of dedicated circuits, the actual bandwidth should be kept as small as possible and only adapted/increased as required. As a minimum, we would provide one channel for the required 64 Kbps signaling. Should I expect any problems?

Answer: Yes, having "dynamic" WAN bandwidth will cause problems that can only be resolved with fixed bandwidth. The reason for this is very simple. Let's assume that the amount of bandwidth currently available is exactly right. Now a call comes through. There is therefore no longer enough bandwidth available. What does the router do? Firstly, it blocks the packets that it can no longer get rid of due to the lack of bandwidth, which affects all connections equally. If the backlog is not cleared within a specific time, it establishes a second 64 Kbps connection in the telephone network. Once connection setup has been completed, there is once again enough bandwidth available. (If not, a further 64 Kbps are set up.) This requires only a few seconds. During this time, all payload connections are affected as is - if not protected by means of prioritization - the signaling connection.

- 17. Question:** How can I check the actual Quality of Service available at an access point? The network operator says that everything is in order. The telephone subscribers complain about sporadic low voice comprehension.

Answer: The QoS values recorded with the real-time transmission protocol can be checked via SNMP at all HG 3575 and HG 3500 boards. See [Chapter 19, "SNMP Support HG 3500 / HG 3575"](#) in the document "HiPath Gateways HG 3500 and HG 3575".

HiPath 4000 Assistant also features an option for recording, evaluating and displaying QoS parameters on a call-by-call basis. See HiPath 4000 Assistant -> Diagnose -> IPDA Service Access -> Call Quality Recording Viewer, MIB Viewer or QoS Viewer

Follow-up question: According to the network operator, not a single IP packet was lost during the period when there were problems with voice communication. Is there another possible cause for poor voice quality?

Answer: If the network operator delivers packets with a delay greater than the size of the jitter buffer, they are not available for the codec when they are needed. This means that although the packets are being delivered correctly from the network operator's point of view, they are lost in the real time context of voice transmission.

18. **Question:** Fax and data via Voice over IP connections are very critical. How well does this really work?

Answer: There are three factors that are relevant here: packet loss, jitter and delay.

Modern voice codecs provide acceptable voice quality even with a packet loss of 5% through procedures such as "packet loss concealment". The packet loss cannot, however, be disguised in the case of fax, modem or ISDN data connections. The throughput declines here due to the number of retransmissions necessary. If packet loss is too high, the connection is cleared down by the terminals.

Jitter causes indirect packet loss. Jitter buffer dimensioning is important here. This should be dimensioned as small as possible to keep delays short. However, packets whose deviation from "normal" delays can no longer be compensated for in the jitter buffer are lost.

The total number of packets lost in the network or due to high jitter levels should be significantly higher for voice than for fax, modem and data.

To satisfy the various traffic type requirements in terms of jitter-specific packet loss (voice < 5%, fax, modem data ~0%), the jitter buffer value set for fax, modem or data connections is increased by 30 ms in the HiPath 4000 components HG 3500 and HG 3575.

The delay on the connection can - depending on the data transfer protocol used - also be critical. If transmission is subject to acknowledgement, the acknowledgement is delayed by the transmission delay which reduces the throughput in contrast to undelayed connections.

The signal processors evaluate the signaling tones from the connected fax or modem devices when setting up a connection. A distinction is made here between high- and low-speed devices and transmission is optimized accordingly.

19. **Question:** What bit rates are guaranteed by IPDA for fax devices or modems?

Answer: IPDA is unable to guarantee bit rates higher than those ensured by the HiPath 4000 central system. That is 14.4 Kbps. Higher bit rates lead to dependencies on the attenuation plan, the attenuation set at the T reference point, etc. Bit rates above 14.4 Kbps are technically possible in particular constellations but cannot be guaranteed.

20. **Question:** The customer uses an all-in-one device (printer/scanner/modem combo) as a fax machine. Fax connections to conventional fax devices work perfectly. Faxes from identical devices within the HiPath 4000 IPDA system, however, cause problems.

Answer: Problems are caused by all-in-one devices that want to improve the transmission speed above and beyond the fax standard. These devices enter the negotiation phase at the start of the fax connection as "normal" Group 3 fax devices. If they both determine that they both support a proprietary - and faster - transmission method, then they use it.

The IPDA gateway problem is like the problem that occurs on remote links. The transmission path is optimized on the basis of the signaling tones that indicate a low bit-rate connection. But the devices decide to use a transmission method with a high bit rate during negotiation. And that causes problems with the path optimized for low bit-rate transmission.

21. **Question:** The IPDA installation works very reliably with over 40 access points. However, it takes much too long to complete startup after the system performs a reload. From a certain point in the time, the system seems to load exactly one access point per minute. What can be done about this?

Answer: Access point startup begins when the standard system startup is complete. The active processor initializes the LAN interface on the SL200 (link LED is extinguished for 1-2 seconds and then lights up again) and immediately tries to set up the signaling connections to the access points. Access points that answer within 70 seconds are loaded at the same time, that is, during the "broadcast". Access points to which this connection could not be set up in time are reloaded individually. When reloading access points individually, one new access point is dealt with every minute.

We have found two reasons why L2 switches block the connection from the SL200 for up to one minute (manufacturer-specific):

- The port on the L2 switch is set to "Autonegotiate".
 - Solution: Fixed bit rate, full/half duplex setting
- The port is configured for spanning tree.
 - Solution: Set the ports to "*portfast*".

22. **Question:** The Service Manual makes repeated references to the pinging of IP addresses for the IPDA components. I'm now doing it, and it only works sometimes or not at all.

Answer: There are three factors that influence a successful ping

- The ping request must reach the destination in order to obtain a response.
For this to happen, the routing from the port of the computer that sends the ping to the destination must be safeguarded. It is therefore important that ping requests come from the IPDA components and not from any other devices on the network (service PC on AP or from Assistant).
- The ping request must not be rejected by a firewall at the destination.
The control processors CC-A/CC-B protect themselves from floods of ping requests by allowing only a specific volume of requests per unit of time. The filter is set up so that a standard ping command with approximately 5 requests in intervals of about one second can be responded to without any problems. However, requests that are more frequent or at shorter intervals are rejected.
Please note also that ping requests are only answered by the currently active processor.
- The ping response must come back to the requestor to be analyzed.
For this to happen, the routing from the pinged IPDA component to the computer that sent the ping must be safeguarded.
The control processors CC-A/CC-B use only host routes to the configured devices (in other words, no general route to the networks on which the devices are connected) and have no default router in the HiPath 4000 LAN segment.

23. **Question:** I want to check the accessibility of the survivability modem at an access point and have pinged the survivability address of the access point (SURVNET+LTU number). The test always fails. However, signaling survivability still works when I release the LAN connection.

Answer: This is due to the fact that there is no route to the address you have used. In the survivability router there is a route for APIPAADDR, which contains the address used by you as the next hop router. Please refer to [Section 4.5.6, "Configuring the Router", on page 125](#).

To check whether signaling survivability - and the modem - is functioning, please use TEST-TSU : SURVMOD, LTU Number;

24. **Question:** I have, on a number of occasions and in different error scenarios, exchanged the NCUI boards “cross-wise”. The error is always repeated. This can't be right, can it?

Answer: With the NCUI, cross-wise exchange is very problematic because the local configuration data needs to be changed.

If you just exchange the modules without reconfiguring them, you take the LTU number and the entire configuration of the shelf as well. The central system accesses LTU 17 with the configured IP address. If the NCUI module with this address now actually sits in another shelf, this is now LTU 17.

You should therefore follow the instructions in [Section 4.2.9, "Information on Exchanging HiPath HG 3575 Boards", on page 91](#) of the Service Manual when exchanging modules. Cross-wise exchange is also a module

exchange.

This involves applying the local configuration (with “HiPath 4000 Expert Access”) in exactly the same way as EXEC-USSU: UPDATAP, LTU Number, UL;

25. **Question:** Survivability test in practice: Survivability works immediately if I remove the Ethernet cable from the NCUI board. However, it does not work if I unplug the Ethernet cable at the CC and/or the STMI. How come?

Answer: A functional distinction must be made here between the signaling part and the payload part. As far as “survivability” is concerned, these are dealt with completely autonomously and virtually independently of one another.

Moreover, the “unplug” scenario is special because the boards here clearly detect a loss of Layer-1 (L1) functionality. This is not as easy in higher layers. A number of other methods are implemented for this and are explained in detail in [Section 4.5, “Configuring Signaling Survability”, on page 112](#) and [Section 4.8, “Configuring Payload Survability”, on page 149](#).

Let’s assume you configured signaling and payload survivability and all LAN cables are connected. (*The starting point is the same for the following three scenarios a, b, and c. These scenarios are not interrelated*)

- a) Disconnect the LAN cable at the NCUI

- The active CC notices that contact to the NCUI has been lost and activates the signaling connection using a modem [*signaling survivability*]
- As the LAN-based signaling connection is lost, all payload traffic relationships between the NCUI and all STMIs are disabled for IPDA (HG 3500). *This is the only time a connection exists between signaling and payload survivability.*
- A call from the AP to the host system would now be routed over the CO. [*Payload Survability*]

- b) Disconnect the LAN cable at the active CC

- If a standby CC is available and its LAN connection (L1) is OK, the processor is switched over and the access points remain in operation. See also Question 10 on page 13-354.
- If there is only one CC available, disconnecting the CC from the LAN disables the IPDA system. Without its LAN connection, the CC is unable to reach the survivability router and, therefore, is also unable to use a modem to control the access points.

- c) Disconnect the LAN cable at an STMI

- This does not affect the CC <-> NCUI signaling connections. The active CC does not need an STMI to control NCUIs. [*no signaling survivability necessary*]

- Unplugging the connector interrupts all active payload connections over this STMI.
- The STMI detects that it does not have a functional LAN connection (L1) and is therefore unavailable for re-seizure.
- The next call between the host and the AP (or vice versa) is routed either over another STMI (if available) or the CO. [Payload Survivability]

26. **Question:** I would like to use the same (signaling) survivability network for multiple (two) HiPath 4000 systems. Is this possible?

Answer: There is no requirement that states that the survivability router(s) (Ethernet -> PSTN) may only be used for IPDA survivability. To cope with major WAN crashes, however, sufficient capacity must be reserved for IPDA survivability so that all access points can be PSNT-controlled at any given time.

The following restrictions must be taken into consideration if an individual router supports a number of HiPath 4000 systems as a survivability router:

- A router port on the PSTN side can only be configured with an IP address.
- Consequently, this port can only be assigned to an IP segment.

To support multiple HiPath 4000 systems, you therefore need multiple router ports with PSTN access that are assigned to the various survivability networks in the various HiPath 4000 systems.

Only one survivability network can be supported with only one router port on the PSTN side. All IP addresses of the routers and the access points are defined after setting the network address of the survivability network (class C network). In this way, access point 17 in HiPath 4000 system A and access point 17 in HiPath 4000 system B would be assigned the same addresses in the survivability network. This leads to problems during router configuration which is why this configuration is not supported.

However, a configuration with a common survivability network would work if the different HiPath 4000 systems used different, non-overlapping ranges of LTU numbers for their access points (for example system A: LTU 17..49, system B: LTU 50..99).

27. **Question:** From the customer's perspective, an IPDA access point is a device that features both IP and TDM ports. The use of devices of this kind in the customer network is prohibited for security reasons.

Answer: There is a widespread and logical ban on the operation of PCs that have simultaneous network access to another networks (that cannot be controlled and is not protected by a firewall, etc.) on the LAN. Devices of this kind could be used as "private" gateways in order, for example, to offer a secure dial-in connection to the LAN.

An IPDA access point used as a gateway for voice connections from TDM <-> IP must have access both to the LAN and to TDM ports.

The design of the HG 3575 guarantees a distinct separation between the payload functionality and the signaling functionality.

In the payload part, random TDM <-> TDM or TDM <-> IP <-> TDM connections are set up at the request of the HiPath 4000 central system. The network consisting of the HiPath 4000 central system and the IPDA access points provides a TDM operation that, from the outside, appears closed and features an internal IP network for networking the access points.

If HG 3575 were misused, additional IP connections would be routed from the NCUI, for example via PPP, to TDM connections.

This is not possible because

- the IP stack only responds to a limited number of ports (see [Chapter 20, “IP Ports”](#) in the document “HiPath Gateways HG 3500 and HG 3575”).
- the signaling unit can access the TDM payload

The HG 3575 supports PPP but only for a signaling connection over an **external** modem connected using a serial V.24 interface in the case of signaling survivability.

28. Question: The survivability concept with dial-in router and modem is too insecure for my customer. Specifically, the option for dialing into the HiPath 4000 LAN segment in the company’s central system is not acceptable under any circumstances. What other options are available?

Answer: Signaling survivability is based on the principle of re-routing an existing TCP/IP connection from a LAN/WAN connection to a PPP modem connection.

The following details are important for assessing importance:

1. The HiPath 4000 control unit accesses the AP over the survivability router NOT the other way around.
 - Each activity is driven by the control unit.
 - Only the routing of an existing (end-to-end) connection is modified. The level of intrusion protection is increased by maintaining/ continuing the TCP/IP connection sequence numbers.
2. The survivability router should only be configured for outgoing calls (see [Section 4.5.6, “Configuring the Router”, on page 125](#)).
 - Consequently, it is impossible to dial into the HiPath 4000 LAN segment. This involves a dial-up connection from the HiPath 4000 LAN segment to the access point, not a dial-in connection into the HiPath 4000 LAN segment.

- The router can be configured to route traffic exclusively from CC-A or CC-B to the AP on the dial-up connection (IP address filter).
3. The dial-up connection consciously selects a modem and not a router. This ensures that
- all traffic that was not forwarded by the LAN port is routed by the dial-up connection in the HG 3575.
 - traffic from the HG 3575 is only routed to the HiPath 4000 LAN segment over the dial-up connection.
4. HG 3575 only permits modem-based control,
- if the source is known (pre-configured CC-A/CC-B address).
 - if the connection over the Ethernet interface is affected.

In contrast to assumptions about the “dial-in connection” in the corporate central system’s network, the detailed overview of shows that the actual design combats the risks of a dial-in connection and is therefore considerably more secure.

Follow-up question: This may be so but the customer wants a router (instead of the modem) at the access point.

Answer: The disadvantage of a “dial-in router” at the access point is that traffic from sources other than the HG 3575 can also reach the routers and can therefore be transmitted to the central system. This problem can be circumvented by appropriate router configuration. However, the HG 3575 only accepts a modem connected over V.24 as an input for the signaling survivability connection.

29. **Question:** We measured the mouth-to-ear delay in a voice connection between the HiPath 4000 central system and an IPDA access point. The delay clearly exhibits a very slow sawtooth pattern. In other words, it falls steadily until it reaches a minimum threshold value and then jumps back to a maximum value and then immediately starts to fall again. What causes this sawtooth process and what can be done about it?

Answer: You have no digital trunk interfaces in the access point or do not use these for clocking the HG 3575.

Without synchronization over digital trunk interfaces in the access point, the clock generators in the HiPath 4000 central system and the access point become asynchronous, despite the extremely high precision of the free-running clock generator on the HG 3575 (ISO 11 573 class III, TIA stratum 4, CTR4 and CTR12/13). Nevertheless, the unsynchronized clock generators start to diverge over time. In the scenario you measured, the receiver works with a slightly higher clock frequency than the sender. The IP connection starts with the predefined jitter buffer value. As more data is read than sent, the jitter buffer slowly runs idle. This explains the steadily falling mouth-to-ear delay. When the minimum jitter buffer fill level is reached, time is “inserted” at the receive end during which the jitter buffer fills up again. This explains the

jump to the maximum value.

The converse effect can be observed in the opposite direction. The mouth-to-ear delay climbs steadily until the upper limit of the jitter buffer is exceeded. Time is then “removed” and the jitter buffer is reset to the target value.

You can observe this effect in all devices that transfer data at a constant rate over a long period of time without transfer clock synchronization. A solution for the HiPath 4000 IPDA access points involves synchronizing the central system and all HG 3575 ASCs with a common exchange clock.

30. **Question:** Why are calls from the IPDA to the central VoiceMail server routed over the CO in the case of payload survivability? This doesn't make any sense. Can this be prevented?

Answer: VoiceMail systems are not affected by payload survivability. This is explicitly specified as an exception in the sales release for HiPath 4000 (1st supplement). In this case, calls are not routed over the survivability path (that is the CO).

Link to sales release:

https://netinfo.icn.siemens.de/es/products/product_hipath_4000_v10/product/vf_doku/update/VPI_36_02_HiPath_4000_1_Nachtrag_VD_d.doc

31. **Question:** I would like to make an IPDA system with 10 access points survivable and also install a survivability unit in each access point. Why do I now need trunk access in each access point?

Answer: If the central system or IP network breaks down, your HiPath 4000 is divided into 10 or 11 separate systems. Within these separate systems (islands) you can make calls without any problems. However, you cannot make calls between the islands. Bear in mind that in this case, you also cannot transfer any emergency calls in the CO or to another access point.

32. **Question:** When the central system breaks down, a HiPath 4000 system with IPDA and AP Emergency is divided into 5 islands. Each island is controlled by a survivability unit. Can islands communicate via IP insofar as this is permitted by the IP network?

Answer: No. Each island represents an individual system in emergency mode. These systems only communicate via CO or tie trunks.

Follow-up question: If I configure IP trunking between the islands, will it work then?

Answer: In principle yes, however, you cannot only configure IP trunking for emergencies. It must be configured in the central system and is then also available during normal operation. You must pay particular attention here that you are dealing with tie trunks in normal operation within a system, something that is very difficult to manage in terms of LCR. Therefore, we would strongly advise against such scenarios.

33. **Question:** A HiPath 4000 system with 16 access points in 2 sublocations is equipped with 2 survivability units - one in each sublocation. Is it sufficient if one CO access is available in each sublocation?

Answer: Yes, if the sublocations can be reached via different numbers. If both sublocations use the same number, there is a 50% chance that incoming calls in emergency cases will end up in the wrong island. A tie trunk between the islands via CO is also risky.

You do, however, have the option of prerouting through the carrier.

34. **Question:** Why is the entire access point reset and reloaded when switching from the main system to the survivability unit and vice versa? It could just keep running.

Answer: The survivability unit has no information on existing calls established by the main system and vice versa. These calls could not be activated without restarting the access point.

The configuration and the loadware can differentiate between the main system and survivability unit for a transitional period if a complete backup/restore has not yet been run after changes are made on the main system.

35. **Question:** Why do still I need signaling survivability after AP Emergency has been introduced? I could now make savings on the modems and trunk line requirements.

Answer: AP Emergency and signaling survivability are aimed at different failure scenarios.

AP Emergency cannot replace signaling survivability as all connections are interrupted during switching if the LAN fails. This is not the case with signaling survivability.

If the central system fails, signaling survivability is powerless against it. The features therefore supplement each other.

Index

Zahlen

19" HiPath AP 3500 access point 92, 94

A

Access point 57, 68, 80, 81, 83, 86, 261

Access Point Emergency - Configuration 192

Access Point Emergency Feature Description 18

Access Point Emergency Implementation Scenarios 19

Access point parameters, changing 80

Access Points for AP Emergency 200

Access Points from the AP Emergency Configuration 204

Administration Switchover of APs 210

Allocating Access Points to a Survivability Unit 24

Application Support in Emergency Mode 29

C

Call scenarios 10

CC-AP in HiPath 4000 - configuration / modification 193

CC-AP in HiPath 4000 - Deletion 195

Circuit switching 9

CMI 181

CO trunk circuits in access points 168

Configuration Data 26

Configuring an access point 57

Connection Between Subsystems (Islands) 27

Connection Data 207

D

Deleting an access point 81

Deleting the Entire AP Emergency Configuration 204

Different Time Zones (DTZ) 16

Direct link access point 68

Display for AP Emergency on the optiSet/optiPoint 205

E

Emergency Group configuration / modification 195

Emergency Group Deletion 199

External Music on Hold 176

F

FAQs - Frequently Asked Questions 353

Feature description 7

Feature Licensing 29

H

HiPath 4000 Backup & Restore 216

HiPath 4000 in the Customer LAN 192

HiPath 4000 in the customer LAN 31, 34

HiPath Backup Restore Configuration on the CC-AP 232

HiPath HG 3500 as HG3570 in the HiPath 4000 system 96

HiPath HG 3575 87, 91

I

Information for Network Administrators 304

Information on exchanging HiPath 3575 HG boards 91

IP address changes 182

IP addresses, checking 32

IPDA configuration 37

L

LAN interfaces for the processor modules 31

LCT Configuration 280

Load calculation 241

Loading new loadware on a HiPath HG 3575 87

Local Access Point Administration at CLI via Terminal 261

Local Configuration of an access point 83

Local Craft Terminal (LCT) at the access point 32

M

Music on hold 176

N

Network administrators 304

Networked access point 58

Normal Operation 25

P

Patches 27

Payload survivability 149

R

Reference clock in access point 86

Reverting to Normal Operation 25

S

Short description to install an AP Emergency (IPDA) 317

Signaling survivability 112

Source-dependent routing 145

Special routes 101

Spreadsheets - IPDA configuration 269

Startup of the CC-AP 223

Subscriber trunk circuits in access points 168

Index

Survivability for signaling and payload 9
Survivability Function (HiPath 4000 V1.0) 18
Survivability Unit 23
Switchover Delay 205
Switchover in Emergency Mode 24
System capacity 8
System Releases 27

T

Tie trunk circuits in access points 168
Time Synchronization 28
Time Synchronization Between the Central System
and CC-AP 212
Transferring New System Releases and Patches 27

U

Unix Configuration on the CC-AP 227

V

Verification and Acceptance of the AP Emergency
Configuration 239