Documentation

HiPath 4000 V5
IP Solutions - HiPath Gateways HG 3500 and HG 3575

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 - HiPath Gateways HG 3500 and HG 3575 - Contents

1 Goal of this Document

This document aims to provide an overview of the new HG 3500 V4 and HG 3575 V4 gateways in HiPath 4000. Only the basic board configuration is described. Detailed information on specific functions such as IP Distributed Architecture and Access Point Emergency (IPDA & APE), HiPath Feature Access (HFA), Large Enterprise Gatekeeper, etc. are provided in the corresponding sections.

2 Terms

2.1 Key Words

In order to prevent confusion, a number of key terms which are used frequently within the text are defined here in more detail.

Nodes: Designates a device with a port/connection in a network.
This can be a router, a HiPath 4000 CGW module or any computer.
Also frequently referred to as “Host“.

LAN segment: Part of a network in which all nodes communicate with each other directly on Layer 2 (Ethernet MAC). The nodes are thus switched on the same “shared“ medium and interconnected via hubs or Layer 2 switches. In other words, they communicate without routers (Layer 3). The communication with nodes beyond this segment has to be realized via routers.

IP address: A numerical Internet address comprising 4 sets of digits, e.g. **172.16.222.45**. In this context, the term always designates the individual, complete and unequivocal address of a node.

Network mask (Netmask): Internet addresses are broken down into network-specific and node-specific sections. The size of these sections differs, depending on the class of the address (determined by the first digit of the address).

Byte	1	2	3	4
Class				
A	Network [1 ..	Node	Node	Node
B	Network [128 ..	Network	Node	Node
C	Network [192 ..	Network	Network	Node

The netmask allows subnets to be generated within a network. Specific bits of the node section are used for the purposes of addressing. The network mask specifies which parts of the IP address are to be regarded as network/subnet sections by means of the specified bits. The remaining digits (bits not specified in the mask) designate the node section.

Network address: In this document, the term network address is used for the entire network **and** subnet part of the IP address.
The network address is yielded by a bit-by-bit AND operation of any IP address with the netmask.

VLAN tagging According to IEEE 802.1 p/q, there are two functions which are controlled using a common tag: the **priority** and the **VLAN ID**. The term VLAN tagging is generally applied once the tag is used - regardless of what it is being used for. The same applies in the case of IPDA. When reference is made to deactivating or activating VLAN tagging (AMOs SIPCO or CGWB: `VLAN`), it is the tag that is meant, not the VLAN function.
According to the standard there are three types of frames:

- Untagged — Normal Ethernet frames without tagging
- Priority Tagged — Ethernet frames with tagging
  The priority bits are used
  The VLAN ID is 0.
- VLAN Tagged — Ethernet frames with tagging
  The priority bits are 0,
  The VLAN ID is > 0.

Some IP equipment vendors only allow priority bits to be used when VLAN ID > 0 is set.
When tagging is being used, the IPDA components always use priority tagging, but allow a setting of VLAN ID > 0
The priority bits are fixed according to the traffic type.
The values are specified in Table 2, “TOS values”.

TOS byte

The **T**ype **O**f **S**ervice byte is a component of the header for all IP packets in accordance with RFC 791.
According to RFC 791 (*Internet Protocol*), the byte is split up as follows (most significant -> least significant bit)

3 bits for precedence	3 bits for priority D-T-R	2 bits reserved for future use
111 - Network Control	**Slight delay**:	
110 - Internetwork Control	0 = Normal, 1 = Low	
101 - CRITIC/ECP	**Throughput**:	
100 - Flash Override	0 = Normal, 1 = High	
011 - Flash	**Reliability**:	
010 - Immediate	0 = Normal, 1 = High	
001 - Priority		
000 - Routine		

According to RFC 2474 (*Differentiated Services*), the six high-order bits are used as DiffServ Code Point (DSCP), while the two least significant bits are reserved.

Some of the values to be set are specified as 6-bit values without the 2 reserved bits, and others as 8-bit values (with the 2 reserved bits = 0).
With IPDA, the entire TOS byte is always specified. The two least significant bits are always set to zero.
A pure DiffServ Code Point must therefore be moved 2 bits to the left or multiplied by 4 in order to obtain the TOS byte setting for IPDA.

IP address																															
172								16								222								45							
1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	1	0	1	1	1	1	0	0	0	1	0	1	1	0	1
Netmask																															
255								255								240								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Subnet																1	1	0	1												
Network address																															
172								16								208								0							
1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Table 2-1

Figure 1 Example: Class B IP address, netmask and network address

2.2 Fax or Modem Transmission and Detection

2.2.1 Without FMoIP

The transmission of fax signals (or audio signals from modems) over IP is generally not without its problems.

- With fax/modem transmission,
  - voice compression and
  - voice activity detection

  must be **disabled**.
- Fax/modem transmission is very sensitive to packet loss in the IP network. The effective packet loss rate in the network must be considerably lower for fax/modem transmission than for voice transmission.
- Fax machines and modems are very sensitive to runtime fluctuations on the transmission path, which is why there must be no automatic adaptation of the jitter buffer.

The IPDA components evaluate the pilot tones of the caller fax machine or modem and then make sure that the connection is optimized for modem transmission.

2.2.2 With FMoIP

As of HiPath 4000 V2.0, the “FMoIP“ (FaxModem over IP) feature is used for the transmission of fax and modem signals over the IP network.

FMoIP improvements

The FMoIP feature provides the following new functionality:

- DMC (Direct Media Connect) for fax/modem calls. This results in a maximum of one IP hop (2 IP/TDM conversions) for fax/modem connections within a local HiPath network. DMC is supported for HG 3500 / HG 3575. This is the major improvement in comparison with the last version, where a switch back to master call was performed after tone detection.
- The DMC endpoints HG 3500 and HG 3575 support G.711 F/M.
- T.38

  T.38 is possible for

  – IP trunking connections (H323 and H323A)

  – SIP trunking connections (SIP-Q and native SIP)

  – DMC connections from/to IPDA

  T.38 is not possible for

  – IPDA master connections

  – HiPath 4000 SoftGate

  IMPORTANT: When connecting a fax adapter to a HG 3500 (SIP subscriber), DMC must be deactivated for this device (only then is T.38 transmission possible).
  If you want nonetheless to connect DMC for this device, the codec must be set to G.711 (fax transmission with G.711, not T.38).

- RFC2833 and RFC2198 for fax/modem tones are supported for HG 3500/75 to transfer the fax/modem signals over IP.
- Enhanced DSP tone detection (incl. tone information transfer based on RFC2833/RFC2198) for HG 3500/75 boards. Supported tones:

  – call initiation tones CNG and CT (calling side)

  – call answer tones ANS(CED), /ANS, ANSam, /ANSam (called side)

Requirements

- Using HG 3530 V2.0 board with AP1120 for fax/modem connection a homogeneous HiPath 4000 V2.0 2nd Intro (as of SMR 8 of HiPath 4000 V2.0) network with all V2.0 boards updated to FMoIP version is required.
- FMoIP Feature is a V2.0 improvement for multiple hops fax/modem scenarios. This improvement through FMoIP can only be used, if all HG 3500/3575 boards are updated to an FMoIP version (as of SMR 10 of HiPath 4000 V2.0 (PRB MSC10614)). Without update of all boards to the FMoIP version, the old (still existing) fax/modem functionality of V1.0 and V2.0 1st Intro network will be applied.Mixed mode for HG 3550 between FMoIP and non FMoIP version implicate a G.711 FM instead of T.38 fax connection in case of low speed fax communication. G.711 FM instead of T.38 increases the utilized IP bandwidth. Using FMoIP version for all HG 3550 boards the T.38 fax connection will be preferred for low speed connections.

Restrictions

- When DMC is not able to reduce the number of IP hops for a connection to one IP hop, there will still be a certain risk of broken fax or modem connections because of the resulting delay, even though a G.711 channel optimized for analog data is chosen.
- Fax/Modem call: only supports basic call, no support for supplementary services initiated on basis of an existing connection, such as consultation call. Support of basic call includes forwarded calls (CFU).
- Interworking between v1.0 boards and v2.0 FMoIP boards is supported, with the restriction that the FMoIP features are not used since v1.0 boards do not support FMoIP functionality.
- Due to the variety of the available modem and fax types on the market, there is no guarantee that all FMoIP scenarios will work with 100% reliability. The different behaviors of the modem and fax types (e.g. tolerance) and the typical IP conditions (jitter, delay etc.) can result in failed FMoIP scenarios.
- Clear Channel has to be disabled via AMO configuration because there is no RFC2833/RFC2198 tone detection for Clear Channel. Each fax/modem call should be configured as a regular voice call (G.711, G.729, ...).

T.38

T.38 is an ITU standard for sending fax messages accross IP networks in a real-time mode.

2.3 Codec Standards

To transmit an analog voice signal over digital paths, it must be converted to a digital signal (and then back again). There are different methods for implementing this codec, each of which offer different levels of voice quality and requires different amounts of bandwidth.

Detailed information on the codec classmarks is provided in Table 20, “Classmark handling for codec type” in the document "IP Distributed Architecture (IPA) and Access Point Emergency (APE)".

2.4 Voice Quality

For the transmission of voice over IP networks, there are three other factors that influence the subjective voice quality experienced by the customer:

- **Delay**

  Occurs in the packetization of voice data (see Figure 2 Packet-by-packet voice transmission) and in the transmission of packets. Compression codecs (e.g. G.729) require processing time. In order to compensate for fluctuations in the packet runtime (jitter), a buffer is inserted on the receiver side (jitter buffer). The size of the jitter buffer also influences the overall delay.

- **Packet loss**

  Packets can sometimes be lost during transmission in IP networks. Fill data must then be inserted on the receive side in place of the required packet data.

- **Jitter**

  Fluctuation of the packet runtime above or below a mean value, see Figure 3 Jitter: variation of the transmission delay. The jitter buffer must intercept these fluctuations. The packet earmarked for use is lost if the deviation from mean value is so great that it can no longer be intercepted by the jitter buffer. The effect is the same as for packet loss in the network.

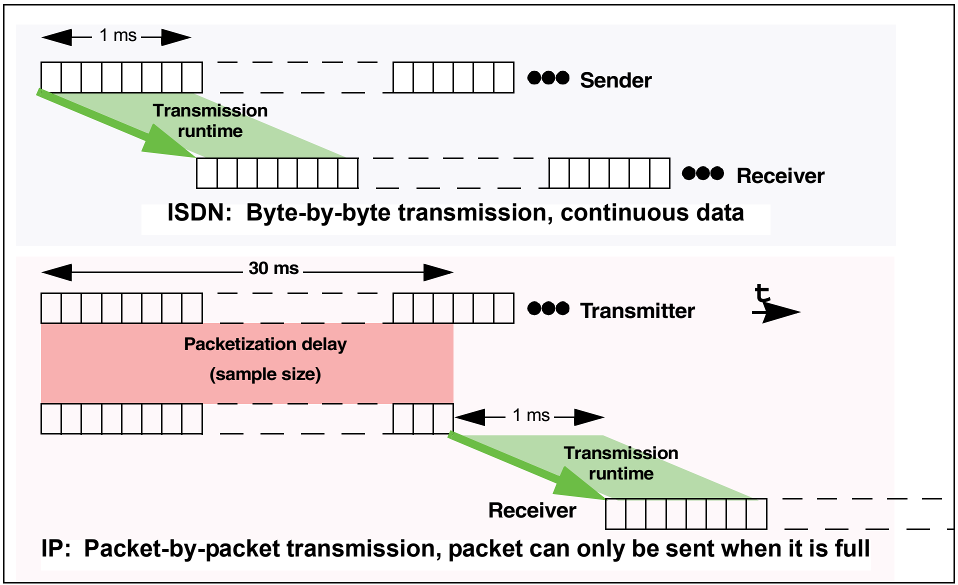

1 ms
Sender
Transmission runtime
Receiver
ISDN: Byte-by-byte transmission, continuous data
30 ms
Transmitter
t
Packetization delay
(sample size)
1 ms
Transmission runtime
Receiver
IP: Packet-by-packet transmission, packet can only be sent when it is full

Figure 2 Packet-by-packet voice transmission

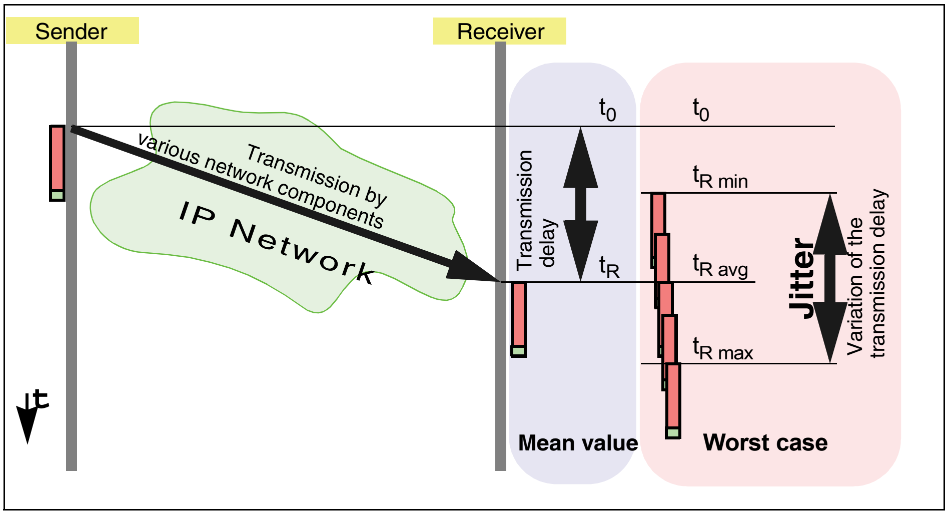


Figure 3 Jitter: variation of the transmission delay

The effectiveness of both parameters also depends on the sample size (how many milliseconds of voice per packet) and on the codec type.

Figure 4 Voice quality depending on delay illustrates an evaluation of voice quality depending on delay.

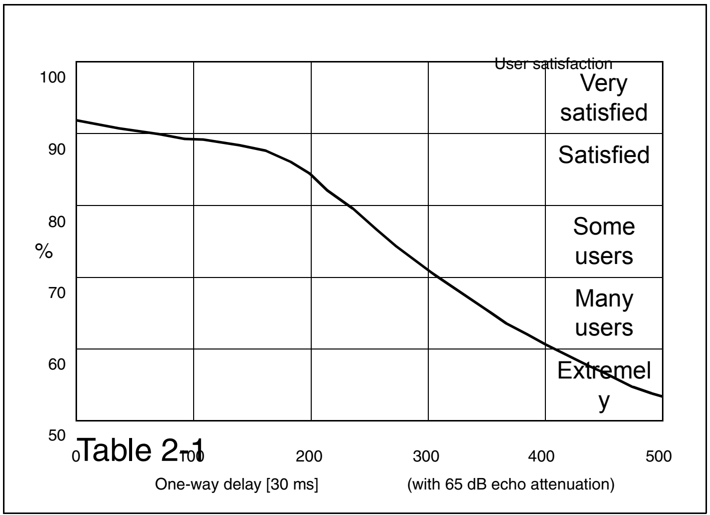


Figure 4 Voice quality depending on delay

Table 1, “Voice quality depending on delay and packet loss rate” illustrates an evaluation of voice quality depending on delay and packet loss rate.

Scale of acceptance	
Value	**Acceptance**
0 - 5	Very good
6 - 10	Good
11 - 19	Satisfactory
20 or more	Unsatisfactory

Delay [ms]	**Packet loss rate in %**						
	< 1%	1%	1.5%	2%	2.5%	3%	> 3%
50	0	4	6	8	10	12	30
100	0	4	6	8	10	12	30
150	0	4	6	8	10	12	30
200	3	7	9	11	13	15	33
250	10	14	16	18	20	22	40
300	15	19	21	23	25	27	45
350	20	24	26	28	30	32	50
400	25	29	31	33	35	37	55

Table 1 Voice quality depending on delay and packet loss rate

For all solutions over IP, i.e. including HiPath 4000, configurations with multiple IP-TDM (or TDM-IP) conversions in a connection should be avoided, as each conversion creates a delay. This is because of the potential losses in voice quality where the number of delays is too high. Every module in the HG 3500 family (and HG 3575 in the access point) as well as every terminal device distributed directly via HFA has a IP-TDM conversion. The maximum number of IP-TDM conversions should (not including HFA terminal devices) be no higher than two.

2.5 Jitter Buffer

2.5.1 Jitter Buffer Functionality

Transfer packets can arrive with different delays in TCP/IP-based networks. Because these delays cause interruptions, packets entering the data stream must be verified. The jitter buffer provides temporary storage for IP packets. It can balance out IP packet delays to a certain degree.

IP packets enter the jitter buffer in the order in which they arrive. Each packet contains a time stamp, which is stored in the RTP header of the packet. The actual order is determined using the packet time stamps. The jitter buffer ensures that packets leave in the right order and in sync. An average time (average delay) defines how long packets, which arrive at the expected time, are held in the jitter buffer. Packets which arrive later than expected are held for a shorter period in the jitter buffer; packets which arrive earlier than expected are held longer. If a packet arrives so late that it can no longer be assigned, it is lost. In theory, packets can also arrive so early that they cannot be assigned. This is, however, rarely the case in practice.

Figure 5 Jitter buffer functionality illustrates the jitter buffer functionality.

If one or two packets are lost during voice transmission, this is not an immediate problem. However, the delay should be as short as possible, as delays which are too long compromise voice quality when making calls.

To ensure data integrity, the number of packets lost during data transfer should be kept to a minimum. Delays, on the other hand, do not play a major role here.

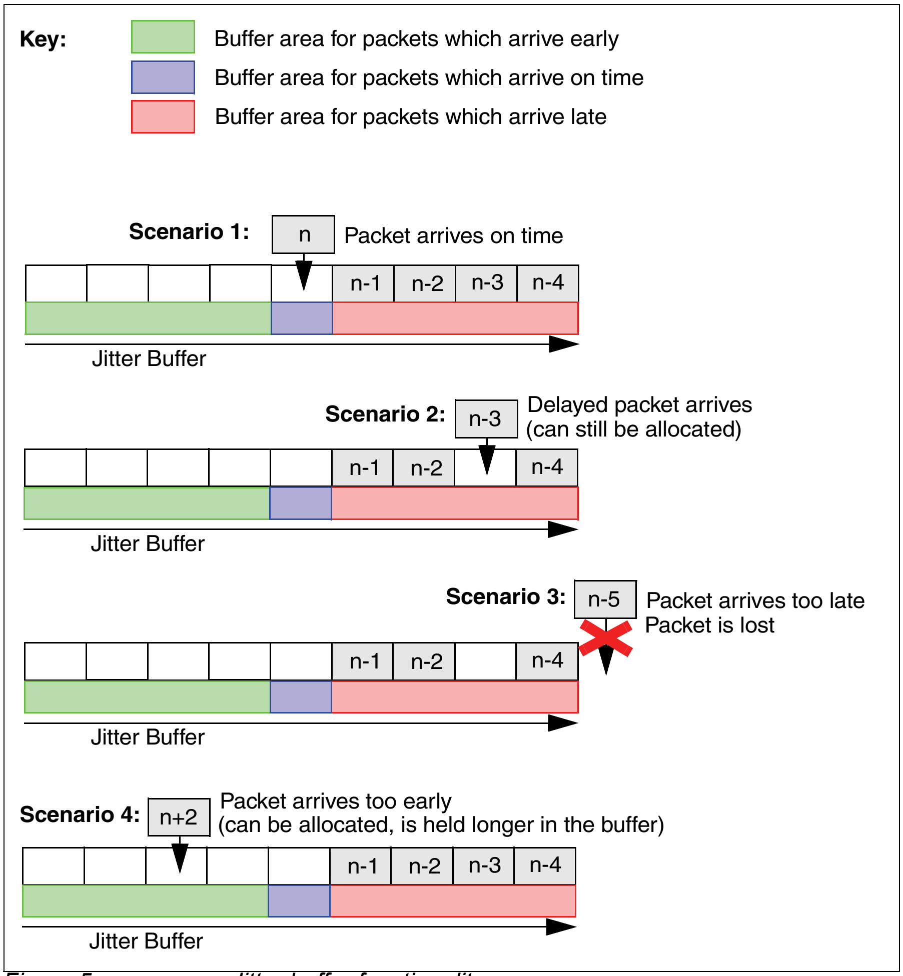


Figure 5 Jitter buffer functionality

2.5.2 Jitter Buffer Modes

As of HiPath 4000 V4, the jitter buffer "Legacy Mode" (JBMODE=0) is no longer supported. If this is still set in the AMO using the parameter JBMODE=0, the static jitter buffer (JBMODE=1) is used regardless, thanks to a mapping in the gateway.

The jitter buffer of the HiPath 4000 gateways HG 3530/50/70/75 can be operated in two different modes, depending on the connection:

- **Static** jitter buffer
- **adaptive** (dynamic) jitter buffer

The adaptive jitter buffer is designed specifically for voice transmission. While the average packet delay remains constant in static mode, it automatically adapts to the situation in adaptive mode. Figure 6 Difference between static and adaptive jitter buffer illustrates the difference between static and adaptive jitter buffers in a situation where several packets with longer delays arrive.

In the adaptive jitter buffer, the average delay is simply the start value for the average delay. This is automatically adjusted to the respective receive ratios during operation (green line).

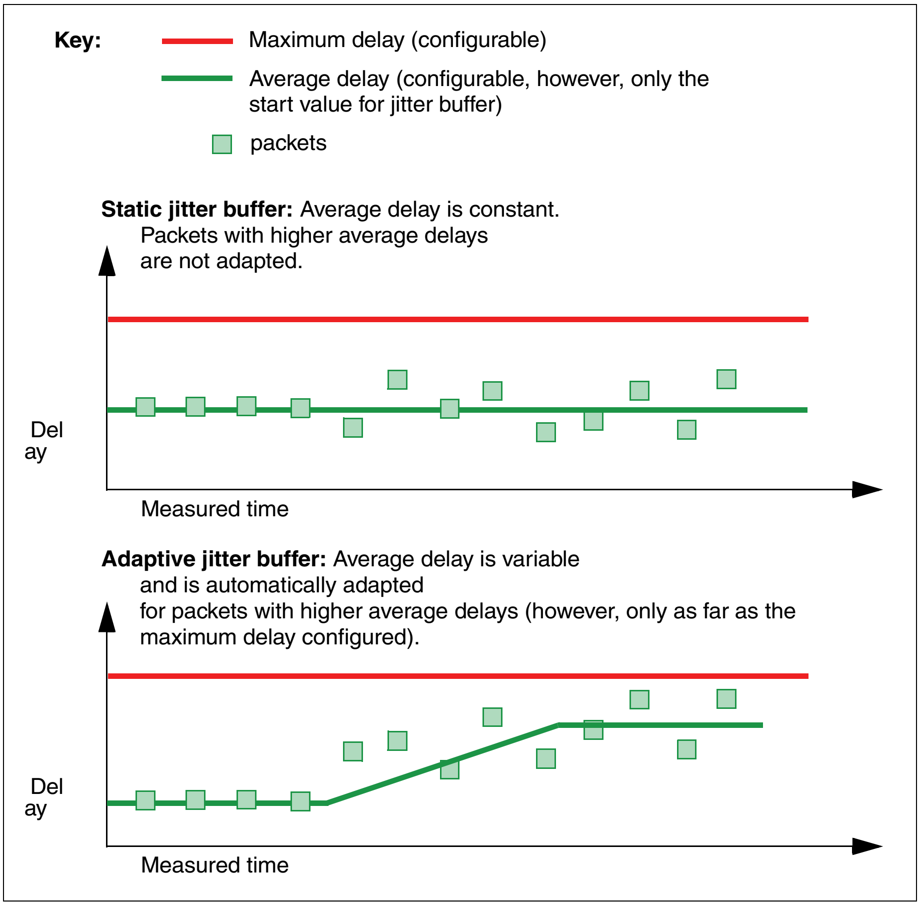

Key:
Maximum delay (configurable)
Average delay (configurable, however, only the start value for jitter buffer)
packets
Static jitter buffer: Average delay is constant.
Packets with higher average delays are not adapted.
Del ay
Measured time
Adaptive jitter buffer: Average delay is variable and is automatically adapted for packets with higher average delays (however, only as far as the maximum delay configured).
Del ay
Measured time

Figure 6 Difference between static and adaptive jitter buffer

2.5.3 Considerations when Configuring the Delay for Static Jitter Buffer

The lower the average and maximum delay is set, the more natural voice transmission will sound to subscribers. However this increases the danger of packet loss and in turn the danger of information loss and distortions. Higher delay values mean less packets get lost, however, it takes longer until a subscriber hears what the other subscriber is saying. Extensive delays can lead to communication difficulties. The following diagram illustrates this:

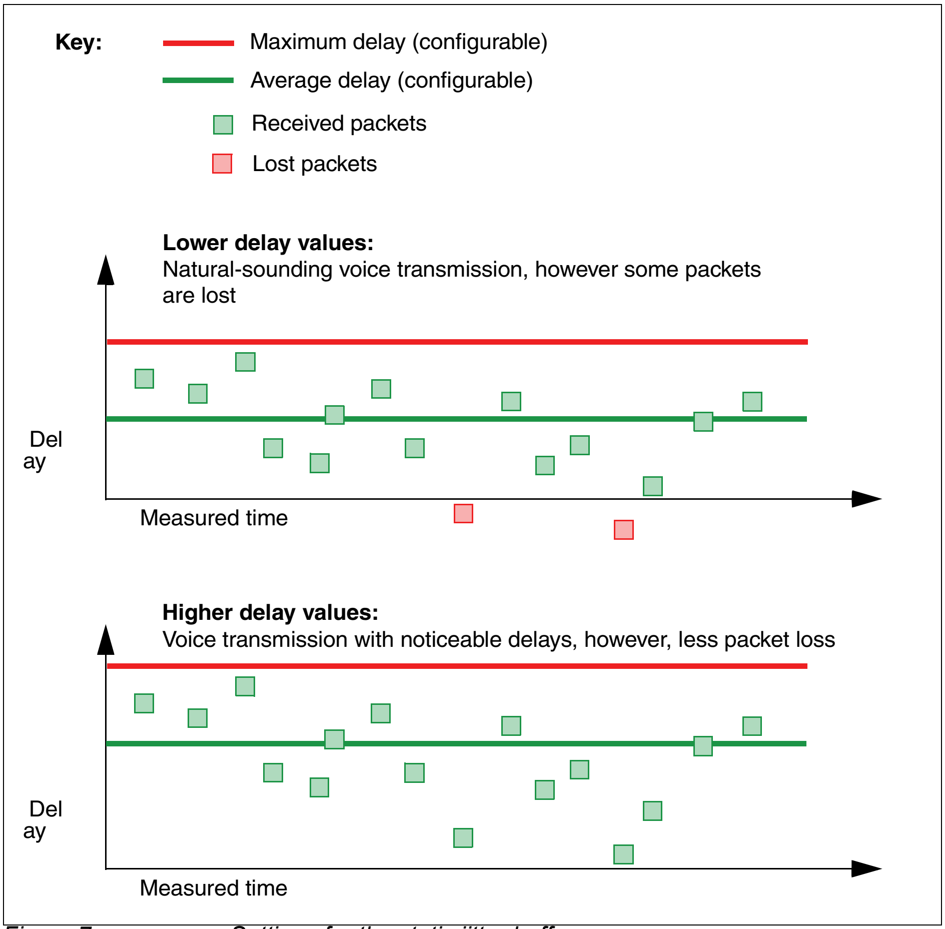

Key:
Maximum delay (configurable)
Average delay (configurable)
Received packets
Lost packets
Lower delay values:
Natural-sounding voice transmission, however some packets are lost
Del ay
Measured time
Higher delay values:
Voice transmission with noticeable delays, however, less packet loss
Del ay
Measured time

Figure 7 Settings for the static jitter buffer

When the HG 3500/75 board is being generated, generous values are set with which most installations will start without any problem. In many cases, these values can then be reduced selectively.

2.5.4 Clock Drift with Static Jitter Buffer

With digital voice transmission in ISDN, all transmission devices operate synchronously. In other words, the volume of voice data per time unit is absolutely the same for the sender and the receiver. For this purpose, transmission devices are synchronized to a common clock pulse (clock signal).

With digital voice transmission over IP, the transmission devices operate asynchronously.
Exception: IPDA access point with digital trunk connection can synchronize with the clock signal.
This asynchronicity means that more or fewer packets are created per second at the transmitting end than are expected at the receiving end. This discrepancy is called clock drift.

If more packets are created at the transmitting end than are expected by the receiver, more packets enter the jitter buffer than intended. This leads to a constant increase in the measured average delay. If this reaches the configured maximum delay value, the jitter buffer adjusts itself. It skips surplus packets until the measured average delay reverts to the set value for average delay. The entire procedure is then restarted. The following figure illustrates the procedure:

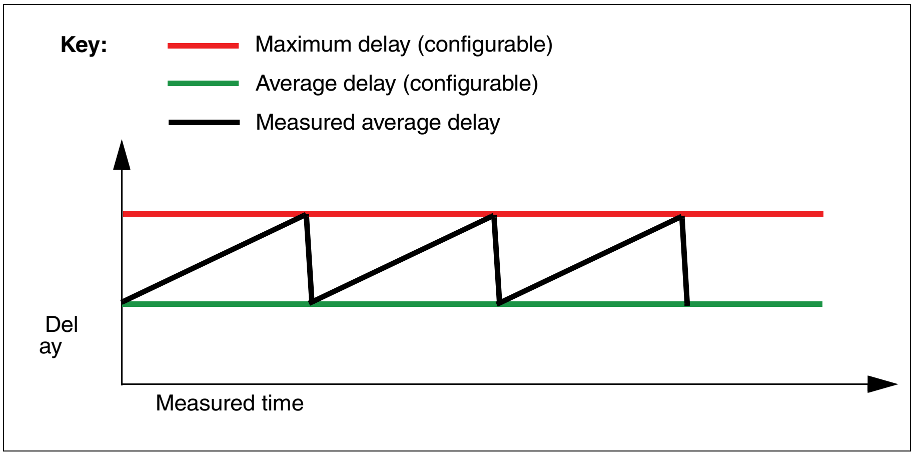


Figure 8 Clock drift in static jitter buffer [transmission quicker than receipt]

If, for example, the average delay is set to 40 ms and the maximum delay to 80 ms, this means that the measured overall delay will increase at intervals by 40 ms from the start value. The length of the interval will be determined by the clock pulse difference of the clock pulse generators in the central system (for all HG 3500 systems) or on the HG 3575 boards as well as on the configuration data (difference between the maximum and the average value). In the sample configuration (40 ms delay hub) the interval is between approximately 30 and 120 minutes long.

If fewer packets are generated at the transmitting end than are expected by the receiver, more packets enter the jitter buffer than intended. This leads to a constant decrease in the measured average delay. If, as a result, the number of packets located in the jitter buffer is reduced to zero, the jitter buffer adjusts itself and resets the measured average delay to the set value for average delay by inserting packets. The entire procedure is then restarted. The following figure illustrates the procedure:

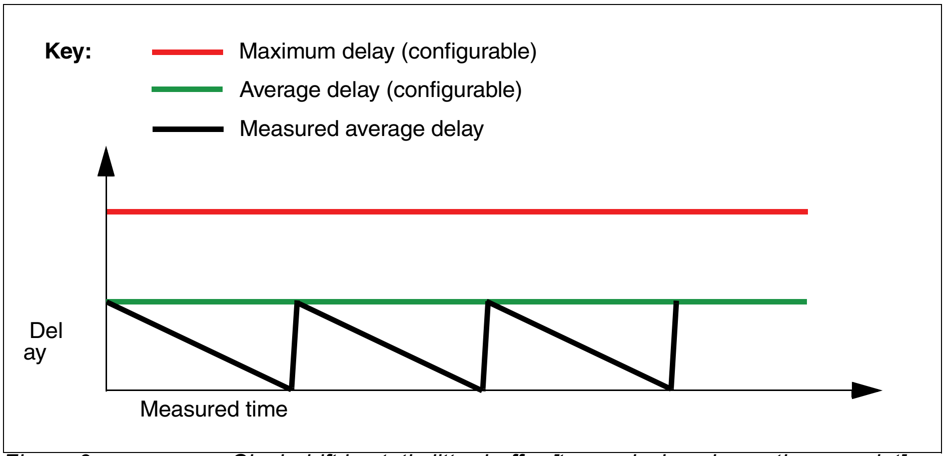


Figure 9 Clock drift in static jitter buffer [transmission slower than receipt]

If, for example, the average delay has been set to 40 ms, this means that the measured overall delay is reduced at intervals from the start value by 40 ms. The length of the interval depends on the clock pulse difference of the clock pulse generators in the central system (for all HG 3500 systems) or on the HG 3575 boards as well as on the configuration data (difference between the maximum and the average values). In the sample configuration (40 ms delay hub) the interval is between approximately 30 and 120 minutes long.

The variation in the overall delay caused by clock drift can be completely avoided by synchronizing the components involved with a common clock pulse.

2.5.5 Minimum Delay for Adaptive Jitter Buffer

In adaptive working mode, the jitter buffer tries to keep the average delay as low as possible. In a situation where no jitter effect occurs, the average delay drops to a minimum. This minimum can be configured in the HG board. The average delay, which is continuously adapted based on the current delay measured, ranges between two values: the configurable minimum delay and the configurable maximum delay. The following diagram illustrates this:

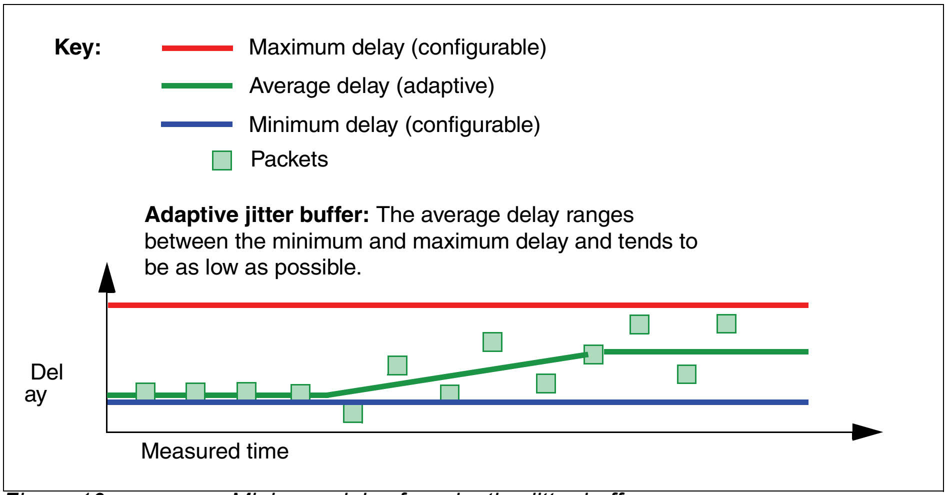


Figure 10 Minimum delay for adaptive jitter buffer

Minimum and maximum delay values are still adhered to if packets are lost.

2.5.6 Packet Loss Control in Adaptive Jitter Buffer

In the case of the adaptive jitter buffer, the average delay is automatically readjusted. The aim of this is to achieve a good balance between having the shortest possible average delay on the one hand and the lowest possible packet loss on the other.

You can set which of these factors is attributed more importance using the “Preference Parameter“. Using values from 0 to 8, you can specify whether decreasing the delay or avoiding packet loss should be prioritized when calculating the average delay. In this case, 0 denotes “Avoid packet loss as far as possible“ and 8 denotes “Maintain shortest possible average delay“. An average value (4) is predefined.

Rule of thumb: setting the value to 0 results in approx. 10 ms longer average delay and setting it to 8 results in approx. 10 ms shorter average delay than that applicable when the average value is set to 4.

2.5.7 Parameters for Jitter Buffer Configuration

To understand the delay parameters, it is important that the values are aligned with the compensable network jitter. As is the case for all IP gateways or terminals, the actual transmission times for voice packets in HG 3500 and HG 3575 also fluctuate around a constant ideal value. This deviation (jitter at transmitting end) is already taken into account during implementation.

These parameters can be set via the **AMO STMIB** (for HG3575) or the **AMO CGWB** (for HG 3500).

- **Jitter Buffer Type:** Select whether the jitter buffer should operate in static or adaptive mode. In adaptive mode, the jitter buffer adjusts the average delay according to the situation when the data is received. In this way, the jitter buffer tries to reduce as far as possible both the delay and the number of lost packets. In static mode, the average delay always remains the same.

- **Average Delay for Voice (msec):** With this parameter you can specify the average number of milliseconds for which an IP packet should be held in the jitter buffer in IP-based voice transmission. In the “adaptive“ jitter buffer, the value specified here only represents an initial value. 40 is the value recommended for most environments.

- **Maximum Delay for Voice (msec):** In the “static“ jitter buffer, this parameter is used to define how many milliseconds are allowed (before the jitter buffer begins to regulate the data stream) for an actual measured delay when IP packets arrive during voice transmission. In the “adaptive“ jitter buffer, the maximum number of milliseconds allowed for the average voice delay is entered in this field. If the actual measured delay is longer, packets are lost. 80 is the recommended value for most environments with the static jitter buffer; 120 is the recommended value for the adaptive jitter buffer. Either way, the value must be higher than that in the “Average Delay for Voice (ms)“ field.

- **Minimum Delay for Voice (msec):** If the “adaptive“ jitter buffer was selected, use this parameter to enter how many milliseconds are allowed for the minimum average voice delay. This means that in every case, the average delay value is higher than or equal to this value.

- **Packet Loss / Delay Preference:** In the case of adaptive jitter buffers, you can use values from 0 to 8 in this parameter to specify whether you would prefer packet loss or a longer delay in the case of large packet delays. 0 denotes minimum packet loss and acceptance of delays in the voice data stream, 8 denotes minimum delay in the voice data stream and acceptance of packet loss. 4 is the value recommended for most environments.

- **Average Delay for Data (msec):** With this parameter, you can specify the average number of milliseconds for which an IP packet should be held in the jitter buffer during data transfer. 60 is the value recommended for most environments.

- **Maximum Delay for Data (msec):** With this parameter you can specify the number of milliseconds allowed (before the jitter buffer begins to regulate transmission) for an actual measured delay when IP packets arrive during data transfer. 200 is the recommended value for most environments. A parameter setting does not make any difference for higher values (approx. 200 upwards) because packets then leave the buffer as soon as they are received in full. Values under 100 ms are possible, however they are not recommended for use.

2.6 Runtime and Noticeable Effects

2.6.1 Delay and Echo

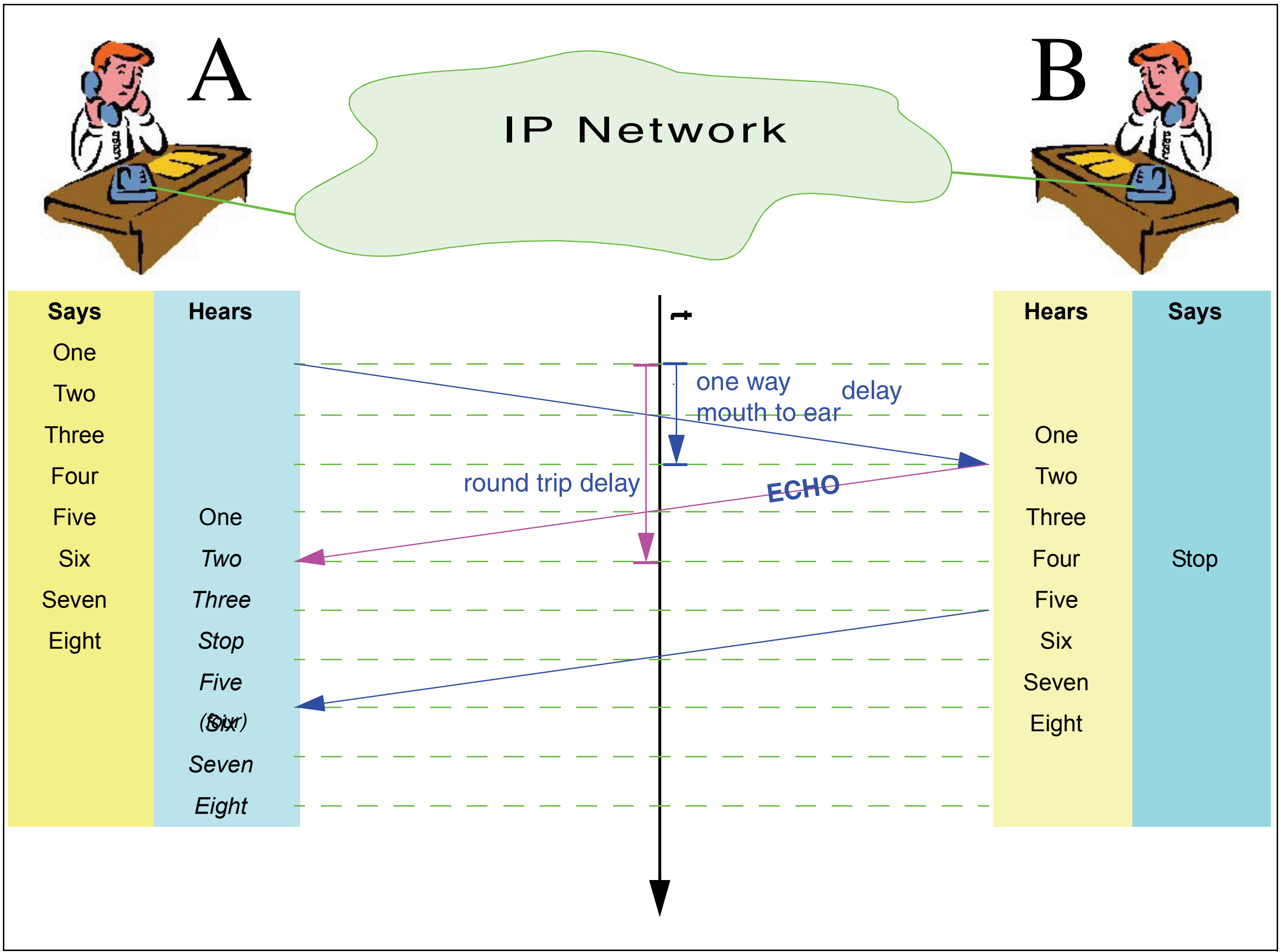


Figure 11 Delay and echo

Voice transmission generally requires more runtime than we are used to in conventional telephony. Figure 11 Delay and echo contains an example illustrating how this sounds. Here the mouth to ear delay is approximately 250 ms.

If Speaker *A* counts from **one** to **eight** and Speaker *B* says **stop** after he hears **three**, *A* hears **stop** while he is saying **eight**. Obviously, selecting a number and saying STOP during counting is not something that happens very often in real conversation. Nevertheless, the delay effect caused by round trip delays is noticeable in normal conversation. It often leads to *collisions* when the speaker changes.

If an echo is generated on the B side (e.g. because of the 2-wire/4-wire hybrid of analog terminal devices, also known as hybrid coil), this is noticed by the speaker, who finds himself speaking over what he said a half a second before, for example.

With high transmission runtimes, it is therefore generally necessary to have echo-free signals on the transmission path. With IPDA, this is achieved through active echo cancellation in the HiPath HG 3500 and HG 3575 modules, which filters out the signal section received from A in the send signal from B (the echo) before transmission of the send signal from B.

2.6.2 Delay and Hands-Free Talking

A common problem is the use of hands-free equipment where there are high transmission delays. Transmission delays are not exclusively generated by IP transmissions. The problem can also be observed with satellite links, for example.

To suppress feedback and echo effects, the hands-free equipment lowers the playback signal in the loudspeaker when a signal is received by the user’s own microphone (automatic gain control). Voice activity prevents the communication partner from being heard. This does not lead to problems in situations where communication is disciplined and the transmission delay is low. Problems arise when the transmission delay is high. Figure 12 Delay and hands-free talking shows how this works. Speaker *A* is impatient and does not wait long enough for an answer from speaker *B* before speaking again. Speaker A’s impatience prevents him from hearing the answer from B which is retarded by the transmission delay. This leads to misunderstandings.

The type of problems caused by transmission delays in hands-free talking are generally linked to the type of hands-free equipment used. Half duplex hands-free equipment (as described) is the most widely used and most sensitive equipment available. Optiset telephones have half duplex hands-free talking. The hands-free setting “noisy room“ is generally the best setting for connection to an IP-based access point (in normal rooms as well).

Optipoint telephones with full duplex hands-free talking are less likely to be affected by the phenomena described above.

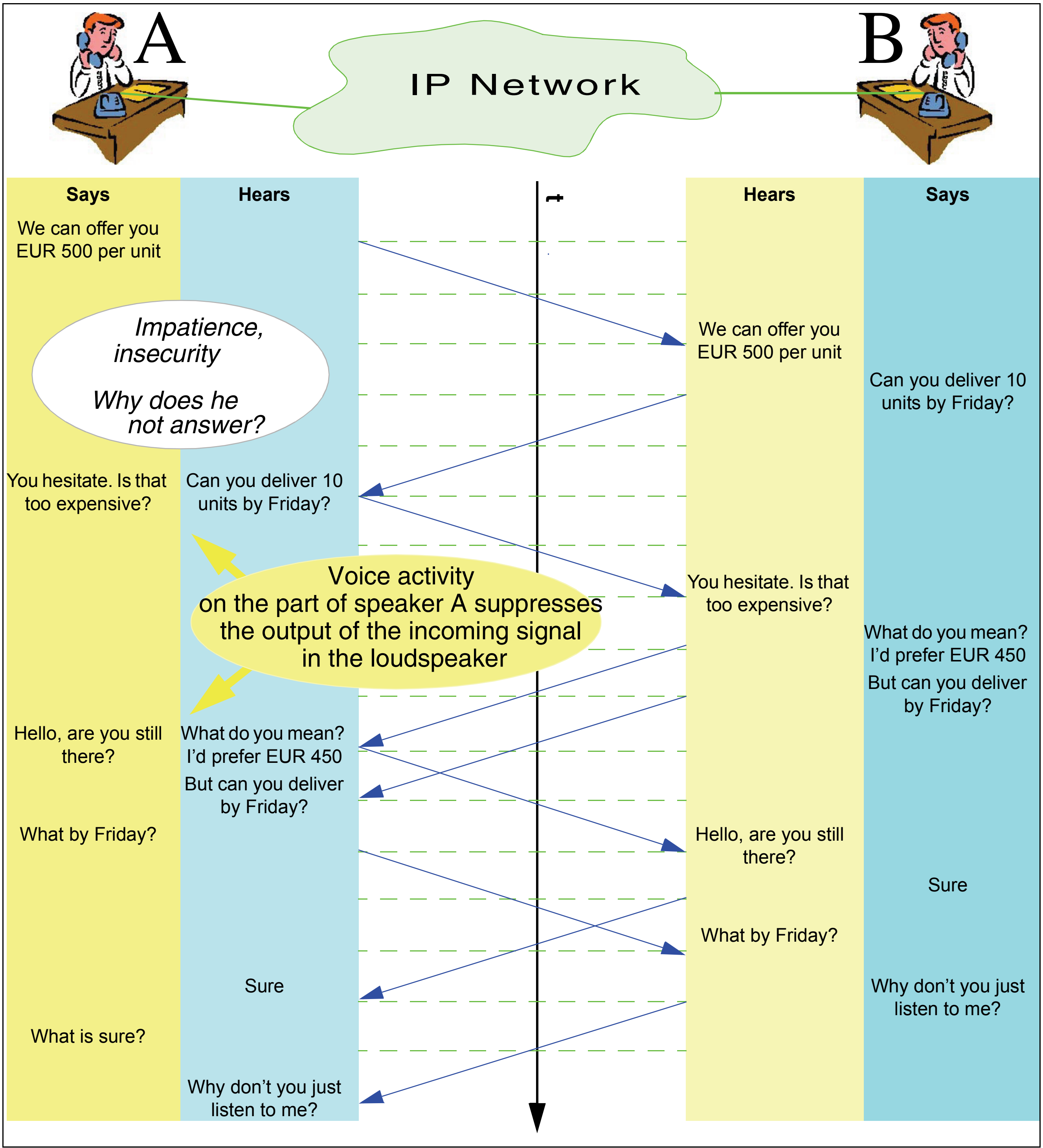

A
IP Network
B
Says
Hears
t
Hears
Says
We can offer you EUR 500 per unit
Impatience, insecurity
Why does he not answer?
We can offer you EUR 500 per unit
Can you deliver 10 units by Friday?
You hesitate. Is that too expensive?
Can you deliver 10 units by Friday?
Voice activity on the part of speaker A suppresses the output of the incoming signal in the loudspeaker
You hesitate. Is that too expensive?
What do you mean? I'd prefer EUR 450
But can you deliver by Friday?
Hello, are you still there?
What do you mean? I'd prefer EUR 450
But can you deliver by Friday?
What by Friday?
Hello, are you still there?
Sure
What by Friday?
Sure
Why don't you just listen to me?
What is sure?
Why don't you just listen to me?

Figure 12 Delay and hands-free talking

2.7 Voice Encryption Devices

Voice encryption devices such as the optiset privacy module, for example, transmit encrypted voice in the same way as modems. The same rules that apply to fax and modem connections apply in this case. The changeover from unencrypted to encrypted mode does not normally take place until there is a call, which is why automatic pilot tone detection is particularly useful here.

3 Architecture and System Requirements

3.1 Prerequisites

Prior to installing IP line gateways at a customer site a network assessment is required that will determine whether the customer's IP network is capable of supporting IP phones. This network assessment will analyze the IP network and determine parameters like jitter, packet loss, available bandwidth, supported QOS mechanisms and assess overall VoIP readiness.

3.2 Power Requirements

The HG 3500 line gateway is a standard HiPath 4000 card that plugs into standard HiPath 4000 enclosures (AP 3300 and AP 3700 Access Points). However, HG 3500 cards require more than average power due to components with high power demands (DSPs). This limits the total number of HG 3500 cards to a maximum of **6** cards per AP 3700 IP (9 slot) and **10** cards per AP 3700 (13 slot).

3.3 Network Requirements

The HG 3500 / HiPath 4000 IPDA components place high demands on the network via which they are coupled to their IP endpoints. Just like signaling links between the CC and the access points, Voice-over-IP data streams are sensitive to packet runtime, runtime variance (jitter) and packet loss.

The availability and reliability of a HG 3500 / HiPath 4000 IPDA system depends heavily on the quality of the IP network used.

Therefore, the network must be examined prior to installation with regard to its suitability for VoIP for the use of HG 3500 / HiPath 4000 IPDA. More details can be found in the HiPath Network Analysis Guide.

All HiPath 4000 components **must** be connected to their own ports on Layer 2 switches.

Using hubs together with HiPath 4000 can cause problems. For this reason, they are not permitted for use in corresponding VoIP scenarios. If hubs are available, they should be replaced with a switch.

In order to achieve a high Quality of Service (voice quality/real time behavior of signaling), the support of IEEE 802.1 p/q VLAN Tagging and IETF RFC 2474 DiffServ is recommended (see Section 3.4, “Network Data”).

IMPORTANT: If an access point is connected over **W**ide **A**rea **N**etworks in which the available **bandwidth is extremely restricted**, the control information (signaling) and voice data (payload) for access points must be given priority over other services.

Frequently, only explicitly familiar TCP/IP or UDP/IP port numbers are supported in the customer LAN for security reasons. All others are then blocked in such cases. Precisely which port numbers must be supported for the HiPath HG 3500 component in the network is described in Chapter 20, “IP Ports”.

3.4 Network Data

This feature is used to configure additional nodes/IP gateways in the customer LAN. Every node/IP gateway requires configuration data which must be coordinated with the network administration of the customer, documented and configured precisely as agreed.

The following data must be specified for every new node/IP gateway in the customer LAN:

- IP address of the node
- Netmask for the network in which the new node is added
- Default router via which the other networks can be reached

Furthermore, the way in which Quality of Service is supported must be clarified for all networks in which HiPath 4000 components are installed. As HiPath 4000 supports IP distributed architecture processes for controlling the Quality of Service in a network on various protocol layers, the following must be clarified:

- Is IEEE 802.1 p/q VLAN Tagging (Layer 2) supported?

  To this end, it is crucial that all network components with which a HiPath 4000 component communicates must support the standard and be configured accordingly. If the network contains nodes (particularly switches and routers) which do not support IEEE 802.1 p/q, VLAN tagging must remain deactivated. The traffic type is assigned a fixed priority value.

- If DiffServ pursuant to RFC 2474 is supported, which CodePoints can be utilized?

In the HiPath 4000 components, TOS bytes must be set to partially differing values for the following traffic types. The default values assume DiffServ support on the part of the network and realize the Quality of Service strategy of Siemens AG.

IMPORTANT:
The TOS byte can be read in a number of different ways:
- Two 3-bit values for precedence and priority
- One 6-bit value as a combination of both 3-bit values (DiffServ CP)
- The entire TOS byte including two fill bits

For IPDA, the entire TOS byte is specified. The two least significant bits are always set to zero. See also Section 2.1, “Key Words”.

Type	Traffic type	HW	TOS byte				IEEE 802.1 p/q Priority
	Package Handling Behavior How should packages of this traffic type be handled?		With DiffServ CodePoint (default)		Without DiffServ		
			Binary	Dec	Binary	Dec	
TOSPL	VoIP payload	HG 3500	0011 0000 (EF)	184	0001 0000	16	5
	Minimal delay Slight packet loss						
TOSSIGNL	Signaling between HiPath 4000 and access point	HiPath 4000	(AF31)	104	0001 0100	20	3
	Minimal packet loss Slight delay						
TOSLAN	Signaling via LAN	AP	(AF31)	104	0001 0100	20	3
	Minimal packet loss Slight delay						
TOSMODEM	Signaling via Survivability connection		0101 0000 (AF22)	80	0001 0000	16	- N/A, as PPP connection
	Minimal packet loss Slight delay						

Table 2 TOS values

The values for **TOSSIGNL** (AMO CGWB, AMO SIPCO), **TOSLAN** (AMO STMIB) and **TOSMODEM** may not be zero. **TOSLAN** and **TOSMODEM** must be set differently to each other. TOSPL is set in AMO CGWB, AMO SIPCO and AMO STMIB.

It is important that the required behavior *(Package Handling Behavior)* is achieved in the network. The absolute numerical values for TOS and IEEE 802.1 priority are not important in this case. They are used solely for the purposes of identifying the required Package Handling Behavior.

The values given in the table are the default settings of the loadware. These settings fulfil the OSCAR specifiactions. You can change the L2 priority with

WBM > Explorers > Network Interfaces > LAN1 (LAN1) > Edit LAN1 Interface

The values can also be changed via the appropriate AMO.

IMPORTANT: If you change the values for HG 3500 with AMO CGWB you have to reboot the corresponding gateways with AMO BSSU.

There are a number of other common prioritization methods, which are managed in the affected routers:

- Prioritization based on the IP address

  The entire traffic from an interface is given (identical) priority. Traffic from IPDA components can thus be given a higher priority than other traffic by specifying the IP address.

- Prioritization of a port (socket) range

  In this case, the IPDA-specific ports (see Chapter 20, “IP Ports”) are given a higher priority than other ports in the network.

  It is essential that the **signaling** and payload ports be taken into account here. This method is not recommended given the size of the port range for payload.

- Prioritization of specific services (TCP, UDP)

  Although prioritization of UDP traffic, for example, in the network would have a positive effect on the payload, it would restrict signaling (TCP/IP). This type of signaling is therefore **NOT** suitable for IPDA. It impairs system availability.

3.5 Bandwidth Requirements

The actual bandwidth per active payload connection depends on the selected encoding algorithm, the specified sampling time and on the fact if the feature “Signaling and Payload Encryption (SPE)” is activated.

3.5.1 Encoding

For example, the following encoding can be selected:

- G.711 (PCM) with support for Annex 1 (packet loss enhancements) and Annex 2 (Voice Activity Detection with Comfort Noise Generation).

- G.729A voice compresses to 8Kpbs.

- G.729AB with Voice Activity Detection.

IMPORTANT: Note that there is virtually no delay introduced in generating G.711 encoding from TDM voice packets (Algorithmic Delay = 0 ms).

For more detailed information on codecs please refer to Section 2.3, “Codec Standards”.

3.5.2 Sampling Time

Voice needs to be digitized before it can be assembled into IP packets.

For telephony applications, voice is sampled every 125 µs at 8bits. It would not make sense to package each individual 8 bit sample into an IP packet. Instead, for G.711 encoding at least 240 8 bit samples are combined into an IP packet.

It takes 30 ms to acquire 240 voice samples.

The Sampling Time is defined as the time it takes to sample a specified number of voice samples that are sent out in **one** IP packet.

It is obvious that the longer the sampling time, the smaller the IP overhead gets. Thus, in order to minimize bandwidth, the sampling time will have to be increased.

However, increasing the sampling time will increase the overall delay!

IMPORTANT: There is always a tradeoff between minimizing the delay versus minimizing the required bandwidth.

For IP line gateways the sampling time can be set between 10 ms and 90 ms depending on codec type.

3.5.3 IP Overhead

The IP overhead includes the Real Time Protocol (RTP) header, User Datagram Protocol (UDP) header and IP headers as well as the Ethernet framing and additional octets for QOS Tagging. A typical IP overhead value for G.711 is 30%.

3.5.4 Required Bandwidth per Connection

Note that the bandwidth calculation is based on 70 bytes of overhead: RTP (12 bytes), UDP (8 bytes), IP (20 bytes), 802.1Q VLAN Tagging (4 Bytes), MAC (incl. Preamble, FCS, 26 Bytes).

IMPORTANT: Bandwidth requirements assume **Full Duplex** operation! When running Half Duplex, twice the bnadwidth is required.

Bandwidth for active DMC master connections without SPE:

Codec	Sampling Time [ms]	Payload Frames per second	Payload [Bytes]	Total Bytes	Bandwidth [Bit/s]
G.711	10	100,00	80	150	120000
	20	50,00	160	230	92000
	30	33,33	240	310	82667
	40	25,00	320	390	78000
G.729AB	20	50	20	90	36000
	30	33,33	30	100	26667
	40	25,00	40	110	22000
	60	16,67	60	130	17333
G.723	30	33.33	24	94	25067
	60	16,67	48	118	15733

Table 3 Bandwidth for active DMC master connections without SPE

Bandwidth for active DMC master connections with SPE:

Codec	Sampling Time [ms]	Payload Frames per second	Payload [Bytes]	Total Bytes	Bandwidth [Bit/s]
G.711	10	100,00	90	160	128000
	20	50	170	240	96000
	30	33,33	250	320	85333
	40	25,00	330	400	80000
G.729AB	20	50	30	100	40000
	30	33,33	40	110	29333
	40	25,00	50	120	24000

Table 4 Bandwidth for active DMC master connections with SPE

Codec	Sampling Time [ms]	Payload Frames per second	Payload [Bytes]	Total Bytes	Bandwidth [Bit/s]
	60	16,67	70	140	18667
G.723	30	33.33	34	104	27733
	60	16,67	58	128	17067

Table 4 Bandwidth for active DMC master connections with SPE

Bandwidth for master connections no longer used (without SPE):

Codec	Frame	Packets		Packet Size [Byte]		Bandwidth [kBit/s]	SID[1] relative to Active
	Length [Byte]	Length	Rate	Pure Data	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	1	71	0,6	0,7%
G.729A	2	1000 ms	1,00 /s	2	72	0,6	1,6%
G.723	4	990 ms	1,01/s	4	74	0,6	2,4%

Table 5 Bandwidth for master connections no longer used (without SPE)

[1] rate between active master connections and master connections no longer used

Bandwidth for master connections no longer used (with SPE):

Codec	Frame	Packets		Packet Size [Byte]		Bandwidth [kBit/s]	SID[1] relative to Active
	Length [Byte]	Length	Rate	Pure Data	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	11	81	0,6	0,8%
G.729A	2	1000 ms	1,00 /s	12	82	0,7	1,6%
G.723	4	990 ms	1,01/s	14	84	0,7	2,4%

Table 6 Bandwidth for master connections no longer used (with SPE)

[1] rate between active master connections and master connections no longer used

3.5.5 Voice Activity Detection (VAD)

Voice activity detection conserves bandwidth in the IP network during pauses in speech and can further reduce the required network bandwidth from 50% to 75% (see Section 5.4, “Voice Activity Detection (VAD)” for more details).

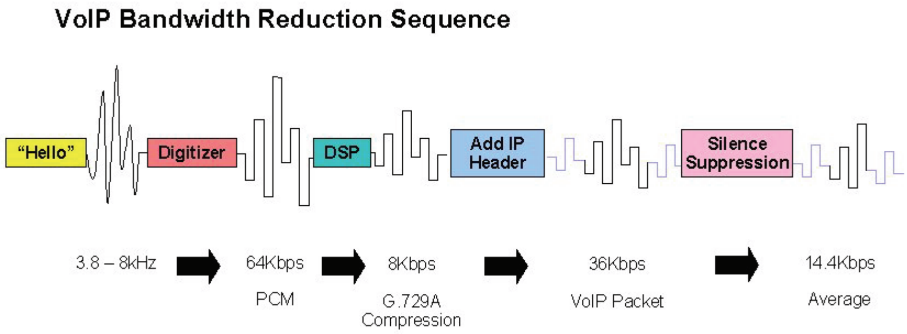


Figure 13 VoIP Bandwidth Reduction Sequence

3.5.6 DMC Considerations

Whenever a DMC connection is established, a "Master Connection" is setup as well.

The master connection is following the same path as the signaling through all the gateways between to IP clients.

The master connection ensures that the necessary resources are always available whenever a feature is invoked that results in a multi party call (e.g. conference). There is also no delay for invoking these types of features because the connection is already setup.

However, there are drawbacks to the master connection concept as well:

- Additional bandwidth is required for sustaining the master connection
- Depending on the configuration significant delays and multiple hops can occur between IP clients when voice payload is using the master connection. Especially when IP end points are located on different IP Access Points on IP connected systems, delays may increase beyond acceptable levels.

In Figure 14 DMC and Master Connection the DMC and Master Connection is shown between two IP networked HiPath 4000 systems for a call between two IP clients (one on each system).

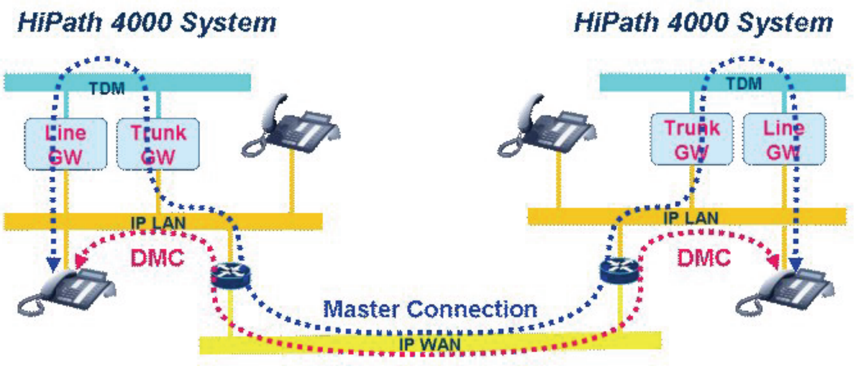


Figure 14 DMC and Master Connection

Enabling VAD will reduce the required bandwidth on the master connection to negligible levels.

Note that delays for each TDM to IP conversion accumulate. In the example above the master connection goes through 3 hops which will result in approximately 200ms end to end delay assuming G.711 encoding with 30ms sampling time and a high quality network (20ms delay). The DMC connection goes only through one hop resulting in an end to end delay of about 80ms.

For more details please refer to Section 5.2, “Direct Media Connection (DMC)”.

3.6 B Channels

The following table provides an overview of the number of available B channels that are dependent on enabled features.

	Relative			STMI2/NCUI2+		STMI4/NCUI4	
				2 DSP	4 DSP	2 DSP	5 DSP
Standards	100%	100%	100%	60	120	60	120
QDC				56	112	60	120
SRTP	75%	83%	100%	45	90	50	120
QDC+SRTP				42	84	50	120
DMC	75%	83%	83%	45	90	50	100
QDC+DMC				42	84	50	100
DMC+SRTP	56%	69%	83%	32	63	40	100
QDC+DMC+SRTP				30	60	40	100

Table 7 Number of B channels dependent on enabled features

Important Notes

- QDC and QDC+DMC with NCUI2+/STMI2

The AMO allows higher values than mentioned in the table above. But the DSP performance is only sufficient for the number of b channels listed in the table above this means the values have to be adapted manually to the values mentioned above.

- QDC, QDC+SRTP, QDC+DMC and QDC+DMC+SRTP with STMI4/NCUI4

  QDC is not considered in the AMO, this means you can configure higher values with the AMO. But this is not recommended!

- QDC, QDC+SRTP and QDC+DMC with NCUI2+/STMI2

  The AMO allows higher values because of the fact that in the AM only DMC and SPE are automatically considered for channel reduction (see Section 3.6.2, “Automatic b channel reduction”). The number of channels has to be adapted manaul to the values mentioned in the table above.

- DMC+SRTP and QDC+DMC+SRTP with NCUI2+/STMI2

  The AMO allows higher values as mentioned in the table above. This does not lead to any problems because the DSP performance is sufficient.

3.6.1 B Channel Configuration

3.6.1.1 AMO BFDAT

Using the AMO BFDAT, the profile of the board is defined with a maximum number of B channels.

- ADD-BFDAT, parameter **BRDBCHL**

  The parameter **BRDBCHL** determines if a block for a board with 60 or 120 b channels will be configured.

- ADD-BFDAT, parameter **FUNCTION**

  With the parameter **FUNCTION** you can configure the functions of the common gateway (i.e. HG 3500, HG 3530, etc.).

- CHANGE-BFDAT, parameter **BCHLCNT**

  With the parameter **BCHLCNT** you can configure the maximum number of b channels per function. This value must not be higher than the maximum number of b channels possible for this funtion (see Section 3.6.1.2, “AMO BCSU”, parameter **BCHLCNT**).

3.6.1.2 AMO BCSU

The profile configured with AMO BFDAT (maximum number of b channels (**BRDBCHL**) and configured functions (**FUNCTION**)) is evaluated by AMO BCSU. Additionally the activated features in the system (i.e. DMC, SPE) will be considered. An automatich b channeld reduction will be performed (see Section 3.6.2, “Automatic b channel reduction”).

With DISPLAY-BCSU the following information can be found:

- How many b channels are available on the board (**BCHANNELS**).
- How many b channels have been configured wit AMO BFDAT per function (**BCHANNELS**).
- How many b channels are possible per function (**BCHLCNT**). The parameter **BCHLCNT** depends on what feature has been activated (see Section 3.6, “B Channels”). The value in parameter **BCHLCNT** can be lower than the configured number of b channles for this function in AMO BFDAT. But only the amount of b channels of parameter **BCHLCNT** are available for the function.

In the case of bandwidth problems, etc. the current value of the B channels that can be used for each configured function must be reduced. This can be done in AMO BCSU with the b channel parameters (i.e. **BCHL3530**, **BCHLSIP**, **BCHL3550**).

3.6.2 Automatic b channel reduction

Using the features for signaling and payload encryption (SPE) and also DMC, automatic b channel reduction is performed, i.e. the current values set are reduced by a fixed percentage. This percentage depends on the hardware used.

IMPORTANT: The automatic b channel reduction is not performed with the feature QDC. This b channel reduction has to be done manually referring to Table 7, “Number of B channels dependent on enabled features”.

Board	Maximum number of b channels	Reduction in %		Reduction in b channels	
		DMC	SPE	DMC	SPE
NCUI2+ (Q2305-X35)	60	25	25	15	15
NCUI2+ (2305-X40)	120	25	25	30	30
NCUI4 (Q2324-X)	60	17	17	10	10
NCUI4 (Q2324-X10)	120	17	0	20	0
STMI2 (Q2316-X)	60	25	25	15	15

Table 8 Number of B channels depending on SPE and DMC

Board	Maximum number of b channels	Reduction in %		Reduction in b channels	
		DMC	SPE	DMC	SPE
STMI2 (Q2316-X10)	120	25	25	30	30
STMI4 (Q2324-X500)	60	17	17	10	10
STMI4 (Q2324-X510)	120	17	0	20	0

Table 8 Number of B channels depending on SPE and DMC

This reduction is not only calculated on board level but on function level. This means that the percentage values from above will be calculated per configured function.

Examples for single feature support (STMI2/STMI4):

1. DMC is activated for HG 3550 on Q2324-X510

   DMC activated on Q2324-X510: reduction of the b channels of 17% (= minus 20 b channels)

   => Maximum number of available b-channels: 120-20=**100**

2. SPE and DMC is activated for HG 3550 on Q2316-X.

   SPE activated on Q2316-X: reduction of the b channels of 25% (= minus 15 b channels)

   => 60-15=**45**

   DMC activated on Q2316-X: reduction of the b channels of 25% (of 45 remaining b channels) (= minus 11 b channels)

   => Maximum number of available b-channels: 45-11=**34**

Example for multiple feature support (STMI2/STMI4):

1. SPE is activated for 2 HG 3550 circuits with 40 b-channels on Q2324-X500. The remaining 20 b-channels are configured for HG 3530.

   SPE activated on Q2324-X500 for HG 3550: reduction of the b channels of 17% (of 40 b channels = minus 7 b channels)

   => Maximum number of available b-channels for HG 3550: 40-7=**33**

   SPE is not activated for HG 3530. Therefore the 20 b channels won’t be reduced for HG 3530.

2. SPE is activated for 2 HG 3550 circuits with 40 b-channels and HG 3530 for 20 b channels on Q2324-X500.

   SPE activated on Q2324-X500 for HG 3550: reduction of the b channels of 17% (of 40 b channels = minus 7 b channels)

   => Maximum number of available b-channels for **HG 3550**: 40-7=**33**

   SPE activated on Q2324-X500 for HG 3530: reduction of the b channels of 17% (of 20 b channels = minus 3 b channels)

=> Maximum number of available b-channels for **HG 3530**: 20-3=**17**

These reduced b-channel values are the upper limit for path selection.

The B channel number increases appropriately when features are deactivated.

Summary:

In the AMO BFDAT, only the maximum number of B channels can be configured. Using the AMO BCSU, the number of currently available B channels can be displayed and the B channels configured.

The following tables provide an overview of the number of available B channels that are dependent on enabled features.

3.6.3 Displaying the B Channels currently Available/ Configured (possible IP-Based Connections)

The total number of B channels currently in use is shown as usual in the AMO BCSU. However, as of HiPath 4000 V4, the parameter BCHLCNT is no longer provided in the AMO BCSU. This has been replaced by the corresponding **B channel parameter for each function** (BCHL3530, BCHLSIP, BCHL3550, BCHLWAML and BCHL3570). As of HiPath 4000 V4, the AMO BFDAT includes the parameter **BRDBCHL**. This defines the maximum number of B channels for the board (60 or 120 B channels).

Using the AMO BCSU, you can query the number of B channels available for the common gateway board. The AMO UCSU must be used for configured HG3575 boards.

IMPORTANT: Determination of the B channel values differs for HG 3500 and HG 3575.

You can check the channels or bandwidth used with the AMO GKTOP following appropriate configuration.

Details on bandwidth management for gateways can be found in the Resource Manager Service Manual (Complex Solutions under the “Large Enterprise Gatekeeper” feature).

`DISPLAY-BCSU:TAB,1,<LTU Number>;` command shows 3 b-channel values:

- The maximum number of B-channels supported by the board,
- the number of used b-channels per function and
- the maximum possible number of b-channels per function.

3.7 Traffic Considerations

From a trafficking point of view, HG 3500 IP line gateways can be treated like a trunk with either 60 or 120 connections. The number of connections required depends on the number of IP phones configured per HG 3500 and the traffic (C.C.S.) values of these phones. Using a standard ErlangB calculation allows determining the number of trunks/connections that are required on each gateway for a specific configuration.

The tools use a simplified approach and allow 240 standard users and 60/120 high traffic (e.g. call center agents) users on each gateway type. Note that you can mix and match standard and high traffic users but you will be limited to 60/120 users per gateway total. This ensures that call center agents will always be able to seize a line.

Capacities

A maximum of 240 IP clients can be configured per HG 3500 gateway.

Typically a 60 connections gateway is sufficient to serve 240 at 6 C.C.S.. In case the users creating a higher amount of traffic, then a 120 connections gateway will be required.

Call center agents are typically trafficked at 32 C.C.S. and thus require a connection on the gateway for each agents. This will limit the number of call center agents to 60 or 120 depending on the HG 3500 type (60/120 connections).

IMPORTANT: Mixing of regular users and call center agents on the same card is possible. However, in order to guarantee connection availability to call center agents at all times, regular users will be trafficked at 1 Erlang (36 C.C.S.)

4 Supported Gateways

The following gateways are supported in HiPath 4000 V5.

4.1 HG 3500 V4 (Common Gateway)

HG 3500 V4 is supported with the following boards:

- STMI2 (Q2316-X and Q2316-X10)
- STMI4 (Q2324-X500 and Q2324-X510)

4.1.1 General Information

- The common gateway HG 3500 V4 consolidates existing VoIP gateways into a single gateway.
- The ommon gateway HG 3500 V4 forms a common architecture for HiPath 4000 V4 and higher based on HG 3550 V2.0 (for HiPath 4000 V3.0).
- All functions provided by the HG 3530, HG 3540, HG 3550 and HG 3570 gateways, including redundancy and load sharing, are retained.
- Support ofthe “mixed“ common gateway. This means that all sub features (trunking, VoIP subscriber, IPDA and WAML) can be used in parallel on a board (**Multiple Feature Support** (**MFS**)). The gateway can also be used as **Single Feature Configuration** (as known from HiPath 4000 V3.0).

  Configuration example for Multiple Feature Support: see Section , “Multiple Feature Support Configuration at the Common Gateway (Example)”.

  Examples of single feature configuration can be found in the documents:

  - HiPath Feature Access (HFA)
  - IP Distributed Architecture (IPDA) and Access Point Emergency (APE)
  - SIP-Q-Trunking / Native SIP trunking or H323-/H323-Annex-trunking

  IMPORTANT: Restriction: Only one trunking protocol may be configured for each board. There are no restrictions on interworking with other functions.

- The HiPath Feature Access (HFA) standby concept will be made available for other functions.

4.1.2 Hardware and Loadware

Until HiPath 4000 V3.0 was released, each feature had separate loadware. This loadware determined the function of the gateway (HG 3530, HG 3540/3550, HG 3570). In HiPath 4000 V4 and later, the various types of loadware are consolidated into a common loadware for STMI2 and STMI4. With this loadware all features are available on a board.

Board	Part number	B channels
STMI2	Q2316-X	60 B channels (2 DSPs)
STMI2	Q2316-X10	120 B channels (5 DSPs)
STMI4	Q2324-X500	60 B channels (2 DSPs)
STMI4	Q2324-X510	120 B channels (5 DSPs)

Table 9 Supported STMI boards

4.1.3 Scenarios and Protocols

Scenarios	Gateway before HiPath 4000 V4	Protocols
IP trunking	HG 3550	H.323
IPDA (host side) - Master	HG 3570	proprietary, under control of SWU
IPDA (host side) - DMC	HG 3570	H.323
HFA subscriber	HG 3530	Cornet-TS
SIP trunking (native & SIP-Q)	HG 3540	SIP
SIP subscriber	HG 3540	SIP

Table 10 Scenarios and protocols with HG 3500 V4

4.1.4 Board Replacement

To replace an STMI board please note the following:

- Replace a “small“ STMI with a “small“ STMI: no problem
- Replace a “large“ STMI with a “large“ STMI: no problem
- Replace a “small“ STMI with a “large“ STMI: no problem
- Replace a “large“ STMI with a “small“ STMI: only works if not more than 60 b-channels are used

Procedure:

- Change the board.

- It is not necessary to delete all circuits on the module and the module itself, but rather to change the part number with CHANGE-BCSU (if necessary).

  ```
  CHANGE-
  BCSU:TYPE=PARTNO,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>,PARTNO1=<par
  t number of board to be changed>,PARTNO2=<part number of new
  board>;
  ```

- Restart the board with

  ```
  RESTART-BSSU:ADDRTYPE=PEN,LTG=<ltg>,LTU=<ltu>,SLOT=<slot>;
  ```

4.1.5 Feature Capacities

Information on feature capacities for both HG 3500 V4 and HG 3575 V4 see Chapter 5, “Features and Restrictions”.

- The HiPath HG 3500 V4 gateway has the capacity to convert 60/120 connections into Fast Ethernet packets and provide TDM to IP conversion for 60/120 concurrent calls.
- HG 3500 V4 gateways can be configured as a **standby gateways** providing backup capabilities in case of individual gateway failure.

More detailed information on standby gateways

One or multiple standby HG 3500 IP line gateways can be defined in the system that will take over in case any of the installed line gateways fails.

This concept is very efficient and cost effective because a single gateway can protect multiple gateways against failure. However, a single gateway cannot protect against multiple gateways failing simultaneously, which is highly unlikely.

In case of a failure, the system will reprogram a standby gateway with the parameters of the failed gateway which will enable the IP clients to re-login and resume standard operation.

IP phones will automatically register with the activated standby gateway and no administrative action is required. Note that users keep the same features and extensions while operating off the standby gateway.

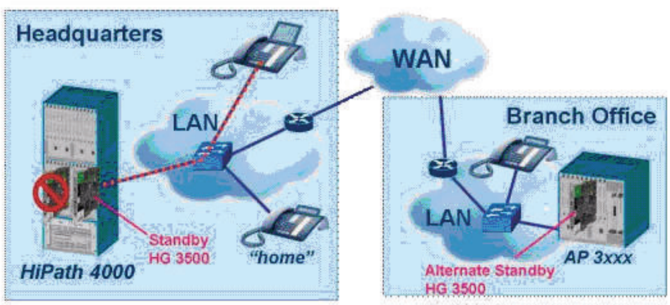


Figure 15 HG 3500 Standby Gateway Operation

Standby gateways can be located in the host system and/or on an IP Access point. The only requirement is that all active and standby line gateways have to reside in the same local IP subnet.

IMPORTANT: Standby gateways and IP clients have to reside within the same system!
E.g.: a standby gateway located in one system cannot control IP clients controlled normally by a gateway located in another system.
Standby gateways at IP Access Points will not protect IP users at the host against a host failure because failures at higher levels (e.g. shelf, AP, host or power failures) will not automatically trigger a switchover.

For configuration purposes please refor to Chapter 10, "Standby Board HG 3500".

- The HG 3500 V4 gateway supports **secondary gateways** that provide full redundancy to IP subscribers. Providing full redundancy for IP clients via **secondary gateways** will protect against higher level failures, like entire Access Point or host failures.

More detailed information on secondary gateways

In order to protect against higher level failures (e.g. Access Point, host failures) secondary gateways can be added to the system. A secondary gateway is an additional, fully configured gateway for an IP client located anywhere within a HiPath 4000 system. Note that each IP user that is backed up via a secondary gateway will have 2 extensions, e.g. x1333 on the primary gateway and extension x5333 on the secondary gateway.

In case communication to the primary gateway is lost (e.g. due to a shelf or host failure), the IP phone will attempt to register with the secondary gateway. As long as the secondary gateway is operational and IP connectivity is available, all phones backed up with secondary gateways will register with their secondary gateway and will be fully operational.

While registered with the secondary gateway the users will have all features available that have been enabled on the secondary extension. Incoming calls terminating on the primary extension will be automatically forwarded to the secondary extension using a new feature called “Alternate Routing on Error”.

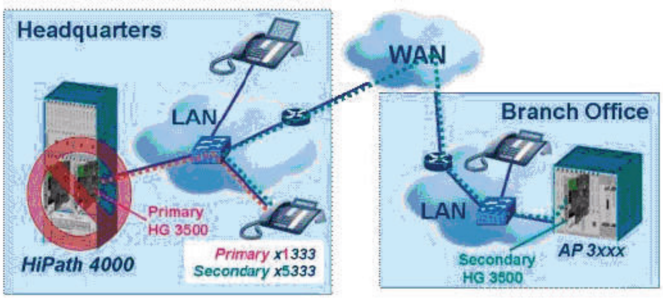


Figure 16 HG 3500 Secondary Gateway Operation

In order to minimize the number of secondary gateways and additional trunks required for operating in failure mode, the following measures can be taken:

- Secondary gateways can be configured with a higher blocking rate, which will limit the number of IP users that can make concurrent calls.
- Minimize the additional trunk required for secondary gateways via “undertrunking”.

Note that these measures are entirely optional and up to the customer’s preference. However, it may be a reasonable approach to limit resources (and thus cost) for operation in failure mode because this is a scenario that is very unlikely to become reality.

IMPORTANT: Secondary gateways and IP clients have to reside within the same system!
Secondary gateways can automatically backup any IP user as long as the secondary gateway is operational and IP connectivity between the IP client and the gateway is available.

- The HG 3500 V4 gateway supports **QoS**. VLAN-tagging according IEEE 802.1p/q on Layer 2 as well as DiffServ (defined in RFC 2474) on the IP Layer have been implemented in order to provide the best possible voice quality using an IP network.

  Of course all switches and routers in the customer’s IP network must support IEEE 802.1p/q and/or DiffServ prioritization in order to take advantage of these mechanisms.

- The HG 3500 V4 gateway supports “**secondary clients**”.

More detailed information on secondary clients

- Secondary clients are optPoint 130 soft-clients configured with the same phone number as a regular IP phone.
- Secondary Clients do not require a ComScendo license.
- Secondary Clients require an optiClient 130 SW license.

The standard H225 Signalling Port is 1720 and this port is used at the OC130 to establish calls from the board to the OC130. For the OC130 Client it might be necessary to use a different port. In the case that an other H323 application is running in parallel to the OC130 it is possible to configure a different H225 Signalling Port on the OC130. The OC130 informs the HG 3500 at registration time and the HG 3500 will use this port for call establishment.

The OC130 can be used as a non standard VPN client. In this configuration the HG 3500 checks the delivered IP address and the real address on the connected CorNetTC socket and informs the OC130 about its real IP address when these 2 addresses are different..

Benefits of Secondary Clients:

- Secondary clients provide **remote** access to all HiPath 4000 features using an optiClient 130 soft client.
- Starting the optiClient 130 on a PC from any location **automatically** logs off the office IP phone (associated by the same phone number) and provides the same feature set and class or service to the end-user as the office IP phone.
- After the remote user returns to the office, the IP phone will still be in the logged off state and the user is prompted to start the phone. This will put the IP phone into a normal operation mode until the IP phone is logged off again by an activation of the associated optiClient 130.

- "**Overbooking**" is possible, meaning that more IP phones per HG 3500 V4 gateway can be configured than there are available connections (maximum of 240 subscribers).

More detailed information on "Overbooking"

For overbooking, more stations (**LINECNT**) are configured than the number of actual subscribers (**BCHLCNT**). The actual number of subscribers is configured for the B channels.

Example:

Five employees are working at a warehouse. However, the warehouse is big enough to house 10 terminals. As only five employees can simultaneously make and receive calls, only five B channels are required.

Parameters: LINECNT=10, BCHLCNT=5

- All IP phones do support **DHCP** and are supported in DHCP mode via the HG 3500 V4 gateway. Note that a DHCP server has to be configured in the IP network; otherwise static IP addresses are required for all clients.
- The **connection of analog devices via a HiPath AP 1120** analog gateway is supported. For more details please refer to the E-Doku pages in the intranet (http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=AP%201120&product_version_main=&product_version_sub=&search_term_type=all&term=&sort_result=title&docclass=&language=&checkdate=&lang=en).
- Full user **mobility** is supported within a single system and networked systems.
- The HG 3500 V4 gateway is supported in all **IP distributed Access Points** including AP 3500/3505 APs that were part of an upgraded v1.0 system.

4.1.6 Impact on Existing Functions

- Impact on analysis options: With the common gateway, all sub features now include comprehensive HG 3550 analysis options.
- Impact on encryption: The common gateway alone no longer supports the HiPath 4000 V3.0 encryption feature. This function will be available again when signaling and payload encryption are released (with Release 1).
- Impact on the standby board concept: Based on the HiPath 4000 V3.0 HFA standby concept in HG 3530, the functional scope of the STMI board is expanded to match that of the HG 3500.

4.1.7 Restrictions

- CQR Viewer

  The CQR Viewer application is only supported for HFA (FUNCTION=HG3530) and IPDA (FUNCTION=HG3570), not for trunking (FUNCTION=HG3550).
- The HG 3500 supports only phone adapters that do not require their own B-channel.

  The following adapters are not supported:

  – phone-adapter,

  – a/b-Adapter,

  - S0-adapter
  - V.24-Adapter
- Autoset Relocate, Teleworking V2.6 and Workstation Protocol are not supported with HiPath HG 3500.
- HiPath HG 3500 line gateways do not operate in a load-sharing mode - there is a fixed assignment of the IP phones to one HiPath HG 3500 gateway.
- The HG 3500 integrated gateway does not interoperate with 3rd party (e.g. H.323/H.450 or SIP compatible) IP phones/clients.
- The HG 3500 integrated gateway requires a static IP address.
- NTP (Network Time Protocol) is not supported on the HG 3500 because there is no real-time clock chip on the gateway card.

4.2 HG 3575 V4

HG 3575 V4 is supported with the following boards:

- NCUI2+ (Q2305-X35 and Q2305-X40)
- NCUI4 (Q2324-X and Q2324-X10)

4.2.1 General Information

- HG 3575 is upgraded to HG 3550 architecture. Basic functionality remains the same. This hub serves as a basis for integrating other possible features.
- In contrast to HG 3500, there is no standby concept for HG 3575.
- The NCUI board is still configured with the AMO STMIB. As of HiPath 4000 V4, configuration is also possible using Web Based Management (WBM).

4.2.2 Hardware and Loadware

New loadware (PZKNCI40) is available for the boards NCUI2+ and NCUI4 in HiPath 4000 V4 and later versions.

Board type	Part number	B channels
NCUI2+	Q2305-X35	60 B channels (2 DSPs)
NCUI2+	Q2305-X40	120 B channels (5 DSPs)
NCUI4	Q2324-X	60 B channels (2 DSPs)

Table 11 Supported NCUI boards

Board type	Part number	B channels
NCUI4	Q2324-X10	120 B channels (5 DSPs)

Table 11 Supported NCUI boards

Board type	Loadware	Restricted B channels	Full feature scope
NCUI2+	PZKNCI40	x	Not possible
NCUI4	PZKNCI40		x

Table 12 Boards, loadware, B channels and feature scope

4.2.3 Exchanging Boards

HiPath 4000 - Access Point

1. Deactivate the shelf

```
DEACTIVATE-USSU:LTG=1,LTU=17;
```

2. Remove the old board, insert the new one

If the new board has the same part number as the old one, proceed directly to Item 6. “Activate the shelf”.

3. Delete the AP

```
EXEC-USSU:ART=DELAP,LTU=17;
```

4. Assign the new part number to the shelf

```
CHANGE-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO=Q2305-X10;
```

5. Configure the AP

```
EXEC-USSU:MODE=CONFAP,LTU=17;
```

6. Activate the shelf

```
ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=17;
```

HiPath 4000 - Switch

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=18,SLOT=99,TYPE=GLOBAL,PATTERN=213;
```

```
CHANGE-
STMIB:MTYP=NCUI2,LTU=18,TYPE=IFDATA,VLAN=NO,TOSLAN=72,TOSMODEM=8
0,VLANID=0,BITRATE=100MBFD;
```

```
CHANGE-
STMIB:MTYP=NCUI2,LTU=18,TYPE=SERVIF,LOGINTRM="TRM",LOGINPPP="PPP
";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,TOSPL=48=PRIO=PRIO1,CODEC=G711
,VAD=NO,RTP="30";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO2,CODEC=G729,VAD=NO,R
TP="20";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NO,R
TP="20";

CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO4,CODEC=NONE,VAD=NO,R
TP="20";

CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO5,CODEC=NONE,VAD=NO,R
TP="20";

CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO6,CODEC=NONE,VAD=NO,R
TP="20";

CHANGE-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO7,CODEC=NONE,VAD=NO,R
TP="20";

CHA-
STMIB:MYTPE=NCUI2,LTU=18,TYPE=JB,AVGDLY=40,MAXDLYV=120,MINDLYV=2
0,PACKLOSS=4,AVGDLYG=60,MAXDLYD=200,JBMODE=1;

CHA-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=SIGQOS,BANDW=0,MAXRTD=0,MINTHRPT=0
,SIGPTHSW=STD,QOSSTAT=NO;

CHA-
STMIB:MTYPE=NCUI2,LTU=18,TYPE=H323,Q931T1=50,Q931T2=500,GWNAME="
HG3575-2";

CHA-STMIB:MTYPE=NCUI2,LTU=18,TYPE=DMCDATA,DMCALLWD=NO,DMCCONN=0;

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=SNMP,CS1="public";

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-
DEVEL",ROLE=ENGR;

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-
SU",ROLE=SU;

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-
ADMIN",ROLE=ADMIN;

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=WBMDATA,LOGINWBM="HP4K-
READER",ROLE=READONLY;

CHA-STMIB:MYTPE=NCUI2,LTU=18,TYPE=GWSECTOR,GWSECTNO=0;

CHA-
STMIB:MYTPE=NCUI2,LTU=18,TYPE=DLSDATA,DLSPORT=10444,DLSACPAS=NO;
```

WBM configuration

Complete additional settings via WBM.

CLI configuration

So that a connection can be established again to the switch, the IP addresses in the new board must be configured via CLI.

5 Features and Restrictions

The following features are supported on HG 3500 V4 **and** HG 3575 V4! For features concerning HG 3500 V4 only please refer to Section 4.1.5, “Feature Capacities”.

5.1 Gateway Functionality

The HG 35xx V4 gateways are only supported in the HiPath 4000 V4 or higher communication platforms.

5.2 Direct Media Connection (DMC)

The HG 35xx V4 gateways support **Direct Media Connection**s (**DMC**).

More detailed information on Direct Media Connections

The HG 35xx V4 gateways support Direct Media Connections (DMC also referred to as peer-to-peer) between two IP phones or an IP phone and an IP board like another HG 3500 or HG 3575. Payload between two DMC endpoints (DMC endpoints = IP phone, HG 3500/3575) is switched entirely in the IP network without involvement or the TDM switching matrix. This ensures highest quality voice and minimal delays because only a single hop (TDM to IP to TDM conversion) is required.

IMPORTANT: Note that invoking any feature that results in a multi party call (more than 2 parties) will route the payload through all gateways in the payload path (same as in HiPath 4000 V1.0). This may result in undesirable delays in certain scenarios (see Section 3.5.6, “DMC Considerations” for more details).

Bandwidth is required for the master connection in addition to the DMC connection. The required bandwidth for the master connection can virtually be eliminated by using VAD for the IP clients. In case VAD cannot be enabled then twice the bandwidth is required.

For more information on DMC and bandwidth please refer to Section 3.5.6, “DMC Considerations”.

5.3 Voice Compression

The HG 35xx V4 gateways support **voice compression** follwoing standard G.711A encoding at 64Kbps. Compression according to G.729A and G.729AB is supported as well. Also supported codecs are G.711U, G.723 (only for HG 300 V4), G.729 and G.729B.

Of course the actual bandwidth requirements per connection depend on the added IP overhead and various other settings (see Section 3.5.4, “Required Bandwidth per Connection”).

IMPORTANT: Note that the voice compression as well as the gateway functionality is performed on DSP modules.

More detailed information on voice compression

Voice compression uses complex algorithms to reduce the bandwidth of the voice signal, for example G.729, to an eighth of the bandwidth required by the original PCM signal. Impairment of voice quality is only minimal in this case.

Voice compression can be problematic when it is applied a number of times in succession. In other words, the original PCM signal is compressed using a specific method, transmitted and then expanded back to a standard PCM signal. Then the whole procedure is repeated on another section. In the worst case scenario, with another procedure. Applying voice compression a number of times, particularly using different compression methods, severely impairs voice clarity and in the worst case scenario it can result in unintelligibility.

The linking of compressed transmission segments - particularly using different methods - must therefore be avoided wherever possible.

Given that all digital speech memory systems for announcements, voicemail etc. also compress speech, this type of equipment must be monitored carefully when used with compressed transmission paths.

Within the HiPath 4000 system, connections to announcement/music on hold devices as well as to conference units are configured without compression in order to guarantee undistorted music or good voice clarity for conferences.

The factors specified in association with voice compression, such as compression to an eighth of the originally required (uncompressed) bandwidth, for example, always refer to the actual voice data. If this data is transferred using IP, the IP packaging, the “protocol overhead“, must also be taken into account. The voice data to be transferred is reduced by the specified factor by means of compression, but the overhead remains the same. The bandwidth required in the IP network is therefore never reduced by the specified compression factor, but instead by a lot less. Always take the values specified in Chapter 6, “Load Calculation” in the document “IP Distributed Architecture (IPDA) and Access Point Emergency (APE)“ into account when dimensioning the bandwidth.

5.4 Voice Activity Detection (VAD)

The HG 35xx V4 gateways support **VAD** (**V**oice **A**ctivity **D**etection).

More detailed information on Voice Activity Detection (VAD)

Voice **A**ctivity **D**etection (VAD) serves to save bandwidth in the IP network during pauses in speech.

Based on the knowledge that only one partner usually speaks at a time, while the other partner listens, the bandwidth seized during a call is only really used in one direction (speaking station -> listening station). In the other direction (listening station -> speaking station), only ambient noise and “silence“ are transmitted. Voice activity detection makes use of this knowledge, interrupts the data transmission and drastically reduces the data rate as soon as silence is detected. As soon as voice activity is detected again, transmission for that direction is immediately re-established (with full bandwidth).

If NOTHING is transmitted on a route, the receiving end generally tends to identify the absence of background noise as line failure and therefore as undesirable. Therefore, depending on the codec used, highly compressed background noise is sometimes transmitted or noise is supplied.

The problem with VAD is the difficulty in distinguishing between *ambient noise* and *silence* in transmission. Ambient noise in the room should fall under the category of *silence*, but softly spoken words should be categorized as *voice*. The impairment (or in the worst case, truncation) of the beginning or end of voice activity in the transition area is unavoidable.

Linking is also a problem with VAD. Using VAD on multiple transmission paths in succession can increase impairment effects. The linking of transmission paths with VAD must therefore be avoided.

The resulting bandwidth reduction is in the range of 50% to 75%.

The VAD classmark is deactivated by default, but can be activated at any time for voice connections.

IMPORTANT: VAD must not be activated in the case of fax, modem and digital data connections!

5.5 Comfort Noise Generation (CNG)

The HG 35xx V4 gateways support **CNG** (**C**omfort **N**oise **G**eneration).

While using **VAD**, the DSP at the destination emulates background noise from the source side, preventing the perception that a call is disconnected.

5.6 Echo Cancellation

The HG 35xx V4 gateways support on board **echo cancellation** (performed on the on-board DSP modules) compliant with the ITU-T G.168 standard.

More detailed information on echo cancellation

Echo arises at all analog 2-wire/4-wire hybrids, e.g. in the hybrid coil of an analog telephone, as well as through acoustic over-coupling of speaker and microphone in the recipient’s handset.

If the runtime between the generation of an audible signal and the manifestation of the echo at the speaker (Round Trip Delay) is very slight, the echo has no interfering effect. However, the greater this runtime, the greater the disturbance of the echo. The runtimes in the case of IP transmission are very high. Thus, echoes are always perceived as extremely disturbing. Therefore, it is important that all signals are free of echo prior to being transmitted in the IP network. The resulting effects of delay and echo are explained in detail in Section 2.6.1, “Delay and Echo”.

Echo cancellation suppresses the echo by filtering it out of the data stream. Echo cancellation should always be used as close to the source of the echo as possible.

The following example is intended to clarify this:

- Subscriber A is connected to Subscriber B via an IP route.
- The terminal device of Subscriber B generates an echo of the signal of Subscriber A.
- The echo is to be suppressed near the source, i.e. in the vicinity of Subscriber B, so that the signal from B to A is free of echo before being transmitted across the IP route.

Echo cancellation (echo suppression) is a very complex operation in digital signal processing, which only has a minimal effect on the transmitted wanted signal (without echo).

Echo cancellation is configured automatically for all circuits, but can be deactivated.

Analog modems and fax machines use complicated phase modulation procedures for data transfer which can be affected by interference caused by echo cancellation.

5.7 Redundant LAN Interface

The feature “Redundant LAN Interface” described in the document "IP Distributed Architecture (IPDA) and Access Point Emergency (APE) Chapter 10, “Information for network administrators” is generally supported. However, if the WAML function is configured, this feature is not supported.

5.8 Security

5.8.1 Access for Administration

Authentication methods are used for access to administration.

In order to protect all files and debug info on the HG 3500, access via LAN to HTTP, TELNET and FTP is disabled per default. Access to these files is only possible via the TAP/service PC through a PPP connection. HTTP, TELNET and FTP are accessible via the service connection. Note that a valid login and password is required for using TELNET and FTP.

5.8.2 Access to SNMP

The acces to SNMP is restricted via read and write Community strings. These Community strings can be configured with the **WBM > Maintenance > SNMP > Communities**.

5.8.3 Security in CorNetTC Registration

The log-on between the IP phones and HiPath HG 3500 is secured via SHA1. The payload and signaling connections are not encrypted.

5.8.4 H.235 Security

When this feature gets activated all messages between the HG 3500 and the IP phones are authenticated. Authenticated messages will contain a Crypto Token element. As Crypto Token handling requires precise time and therefore the local system time is distributed cyclic to the IP endpoints.

For more details on configuration please refer to Section 14.7, “TYPE H235DATA - H.235-Security”.

5.8.5 Connecting IP Gateways to the Internet or via External Providers

The connection of IP gateways to the Internet or external providers reveals a security vulnerability ("insecure" LAN/WAN). An IP or MAC address filter must be set to combat this problem. This can be done via the board’s WBM.

WBM > Explorers > Security > MAC Address Filtering or **WBM > Explorers > Security > IP Address Filtering**.

For a detailed description, see "HiPath 4000 V5, HiPath Gateways HG 3500 V4 and HG 3575 V4, Administrator Documentation" (http://apps.g-dms.com:8081/techdoc/de/P31003H3150M1010100A9/index.htm).

5.9 Resource Manager (RM)

IMPORTANT: The Resource Manager is released for use in standalone systems with HFA and IPDA.
A project-specific release (PSR) is required to use the Resource Manager in a HiPath 4000 network.

In a real, complex IP network the available bandwidth is typically not uniform in all sectors.

The Resource Manager (RM) can administer and monitor the bandwidth for up to 800 sectors in a given IP network.

The RM updates a cluster matrix whenever a call is setup or torn down. The matrix allows determination whether there is a resource shortage in any of the involved sectors. Based on the configured bandwidth and the actual bandwidth a call is either allowed to complete or rejected.

The RM calculates real bandwidth, taking compression settings, DMC, FAX, etc. into account.

5.10 Restrictions

5.10.1 Bit Rate

Problem description:

If Auto Negotiation is set as the bit rate in NCUI4 and STMI4 boards in HiPath 4000 (AMO CGWB, **BITRATE=AUTONEG**) and 100 BRK Full Duplex is permanently set in the administrable peer, the peer does not respond to **AUTONEG** and "LAN message flooding" occurs.

The "LAN message flooding" bug was resolved by the FPGA patch (Senta V11 or higher).

This restriction does not affect STMI2 and NCUI2+ boards.

Recommendation:

100 MB Full Duplex must always be set as the bit rate (AMO CGWB, **BITRATE=100MBFD**).

Half Duplex is set internally for **AUTONEG** in the gateway if the Full Duplex is permanently set in the peer.

5.10.2 Loadware-Update or Reset of the Board

Problem description:

An HG 3500 is configured as a SIP trunking gateway. The parameters for the connection to the Web Based Management of the board (AMO CGWB, parameter **MGNTIP** and **MGNTPN**) and the backup server (AMO CGWB, parameter **BUSIP** and **BUSPN**) have to be configured.

After a reset of the board or after a loadware update the IP addresses (**MGNTIP** and **BUSIP**) are restored but not the port numbers (**MGNTPN** and **BUSPN**). These parameter values are set to the default value (in both cases „0“). Therefore a connection to the backup server cannot be established anymore. The needed configuration data for SIP trunking that has been configured in the WBM and has been saved on the backup server cannot be restored. The SIp trunking connection canniot be re-established again.

Solutions:

Check parameter in AMO CGWB and configure it again:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<number>,SLOT=<number>,TYPE=MGNTDATA,MGNTPN=8
000,BUSPN=443;
```

Or save the configuration data in the local falsh of the board during installation of the board:

WBM > Maintenance > Actions > Automatic Actions > Save Local Configuration for Upgrade

For a detailed description, see "HiPath 4000 V5, HiPath Gateways HG 3500 V4 and HG 3575 V4, Administrator Documentation" (http://apps.g-dms.com:8081/techdoc/de/P31003H3150M1010100A9/index.htm).

5.10.3 Possible IP hops

IMPORTANT: More than 3 IP hops can lead to restrictions in a Voice over IP system, i.e. the delay can be too long and the result is poor speech quality or malfunctioning features.

6 Communication Matrix

Legend for the follwoing tables:

▨	Not possible
🟩	Possible

			HiPath 4000 V1.0				
			HG 3550 V1.1				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V1.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨
HiPath 4000 V2.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨
	HG 3550 V2.0	H323	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨
HiPath 4000 V3.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨
	HG 3550 V2.0	H323	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨

Table 13 Networking with HiPath 4000 V1.0

			HiPath 4000 V1.0				
			HG 3550 V1.1				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V4	HG 3550 V1.1	H323	🟩	■	■	■	■
		SIP	■	■	■	■	■
		Native SIP	■	■	■	■	■
		DMC	■	■	■	■	■
		HFA-Mobility	■	■	■	■	■
	HG 3500 V4	H323	■	■	■	■	■
		SIP	■	■	■	■	■
		Native SIP	■	■	■	■	■
		DMC	■	■	■	■	■
		HFA-Mobility	■	■	■	■	■
HiPath 4000 V5	HG 3500 V4	H323	■	■	■	■	■
		SIP	■	■	■	■	■
		Native SIP	■	■	■	■	■
		DMC	■	■	■	■	■
		HFA-Mobility	■	■	■	■	■

Table 13 Networking with HiPath 4000 V1.0

			HiPath 4000 V2.0									
			HG 3550 V1.1					HG 3550 V2.0				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V1.0	HG 3550 V1.1	H323	🟩	■	■	■	■	■	■	■	■	■
		SIP	■	■	■	■	■	■	■	■	■	■
		Native SIP	■	■	■	■	■	■	■	■	■	■
		DMC	■	■	■	■	■	■	■	■	■	■
		HFA-Mobility	■	■	■	■	■	■	■	■	■	■

Table 14 Networking with HiPath 4000 V2.0

			HiPath 4000 V2.0									
			HG 3550 V1.1					HG 3550 V2.0				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V2.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	HG 3550 V2.0	H323	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	🟩
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	▨
		HFA-Mobility	▨	▨	▨	▨	▨	🟩	▨	▨	▨	🟩
HiPath 4000 V3.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	HG 3550 V2.0	H323	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	🟩
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	▨
		HFA-Mobility	▨	▨	▨	▨	▨	🟩	▨	▨	▨	🟩
HiPath 4000 V4	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	HG 3500 V4	HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		H323	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	🟩
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	▨
		HFA-Mobility	▨	▨	▨	▨	▨	🟩	▨	▨	▨	🟩

Table 14 Networking with HiPath 4000 V2.0

			HiPath 4000 V2.0									
			HG 3550 V1.1					HG 3550 V2.0				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V5	HG 3500 V4	HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		H323	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	🟩
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	▨
		HFA-Mobility	▨	▨	▨	▨	▨	🟩	▨	▨	▨	🟩

Table 14 Networking with HiPath 4000 V2.0

			HiPath 4000 V3.0									
			HG 3550 V1.1					HG 3550 V2.0				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V1.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
HiPath 4000 V2.0	HG 3550 V1.1	H323	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		HFA-Mobility	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	HG 3550 V2.0	H323	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	🟩
		SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		Native SIP	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
		DMC	▨	▨	▨	▨	▨	🟩	▨	▨	🟩	▨
		HFA-Mobility	▨	▨	▨	▨	▨	🟩	▨	▨	▨	🟩

Table 15 Networking with HiPath 4000 V3.0

			HiPath 4000 V3.0									
			HG 3550 V1.1					HG 3550 V2.0				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V3.0	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
	HG 3550 V2.0	H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩
HiPath 4000 V4	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
	HG 3500 V4	HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩
HiPath 4000 V5	HG 3500 V4	HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩

Table 15 Networking with HiPath 4000 V3.0

			HiPath 4000 V4									
			HG 3550 V1.1					HG 3500 V4				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V1.0	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
HiPath 4000 V2.0	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
	HG 3550 V2.0	H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	⬛	🟩
HiPath 4000 V3.0	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
	HG 3550 V2.0	H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩

Table 16 Networking with HiPath 4000 V4

			HiPath 4000 V4									
			HG 3550 V1.1					HG 3500 V4				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility	H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V4	HG 3550 V1.1	H323	🟩	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
	HG 3500 V4	H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩
HiPath 4000 V5	HG 3500 V4	H323	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟩	⬛	⬛
		DMC	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	⬛	⬛	⬛	⬛	⬛	🟩	🟩	⬛	⬛	🟩

Table 16 Networking with HiPath 4000 V4

			HiPath 4000 V5				
			HG 3500 V4				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V2.0	HG 3550 V2.0	H323	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	⬛	⬛	⬛	⬛
		Native SIP	⬛	⬛	⬛	⬛	⬛
		DMC	🟩	⬛	⬛	🟩	⬛
		HFA-Mobility	🟩	⬛	⬛	⬛	🟩

Table 17 Networking with HiPath 4000 V4

			HiPath 4000 V5				
			HG 3500 V4				
			H323	SIP-Q	Native SIP	DMC	HFA-Mobility
HiPath 4000 V3.0	HG 3550 V2.0	H323	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	🟩	⬛	⬛
		DMC	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	🟩	🟩	⬛	⬛	🟩
HiPath 4000 V4	HG 3500 V4	H323	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	🟩	⬛	⬛
		DMC	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	🟩	🟩	⬛	⬛	🟩
HiPath 4000 V5	HG 3500 V4	H323	🟩	⬛	⬛	🟩	🟩
		SIP	⬛	🟩	⬛	🟩	🟩
		Native SIP	⬛	⬛	🟩	⬛	⬛
		DMC	🟩	🟩	⬛	🟩	⬛
		HFA-Mobility	🟩	🟩	⬛	⬛	🟩

Table 17 Networking with HiPath 4000 V4

7 Load Concept for Gateway Boards

7.1 Important Information

- This chapter only describes how to update the loadware for gateway boards.
- To update the system as a whole, use the conventional HiPath 4000 Assistant features Software Transfer (SWT) and Software Activation (SWA).
- To minimize system downtime, you can upgrade the gateway boards first with the load concept described below and then upgrade the system with the Software Transfer (SWT2) and Software Activation (SWA) functions.
- For more information on how to update the system as a whole, see "Implementation Scenarios for Features > Updating HiPath 4000 System Software".

7.2 Notes on IP Gateway Loadware

- Although you can store two loadware images on the IP gateway HG3575, only one of these is the "golden load" that is loaded after a cold start (power off).
- Loadware ID check

  A loadware ID check is performed every time the HG3575 is started and compares the board loadware that is being downloaded with the loadware version on the hard disk (:PDS:APSP/LTG/LGA0/PZKNCI40).

  If the result of the check is negative, that is, if there is a discrepancy with the loadware stored on the HD, then the loadware is transferred from the HD to the NCUI via FTP and then installed/restarted.
- Golden loadware check

  In HG3575, the latest loadware to be downloaded is called "golden loadware" (as-delivered NCUI2+/NCUI4 boards include loadware in the flash memory).

  The golden loadware check is always performed after new loadware is downloaded/restarted (loadware upgrade/loadware ID check negative). If this check is successful, the download pointer is rewritten as appropriate so that the golden loadware corresponds to the new loadware.

7.3 New Load Concepts

Load concepts have been improved to reduce the time needed to download new loadware for IP gateways (as of HiPath 4000 V4).

Load concept for HG 3530/HG 3540/HG 3550/HG 3570 in HiPath 4000 V1.0/ V2.0/V3.0

When starting up an STMI board, the board is loaded via the backplane (HDLC) if newer software is available. The board is not in service during loading. The loading time changes depending on various functions. Loading takes between 4 (HG 3530) and 10 (HG 3550) minutes approximately.

Load concept for HG 3500/HG 3575 in HiPath 4000 V4 and higher

- The loadware for HG 3500/HG 3575 is loaded via HTTPS (see Section 7.4, “Updating Loadware with Web-Based Management” and Section 7.5, “Updating Loadware with "LW Update Manager"”).

- Loadware can be loaded in the background during normal operation, that is the activation of new loadware can be delayed (until off-peak hours). The new loadware should nevertheless be activated as quickly as possible to avoid problems.

- Optimized loading for HG 3500 gateways

  As the common gateway development has combined the software of all previous gateways (HG 3530, HG 3540, HG 3550 and HG 3570) in a single software/loadware package, the size of the software has increased accordingly. This has increased the loading time to approximately 15 minutes. The load concept for STMI loadware was adapted in response to this change.

  There are two CGW-STMI2 boards and two CGW-STMI4 boards. These boards all have a different HW ID but share the same loadware in HiPath 4000 V4 and higher. Up until now, loadware had to be downloaded separately for boards with different HW IDs. This was because each board had its own loadware. The new, optimized methodology for CGW-STMI boards means that the loadware is only downloaded once for these boards, even if they have different HW IDs.

  This results in the following implementation scenarios:

  - Configuration featuring both STMI4 types and an STMI2 type => loadware is only transferred once and then distributed to all corresponding boards.

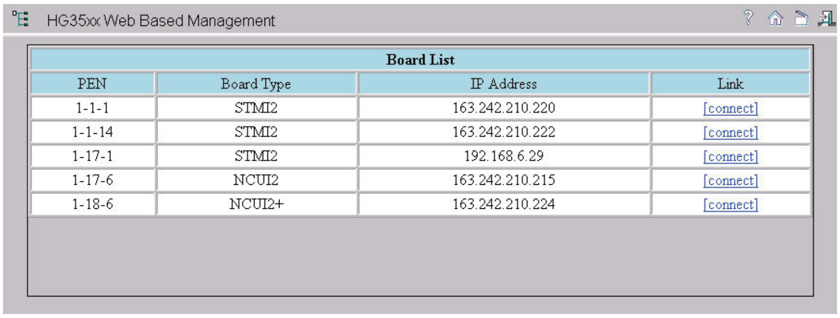
  - Configuration featuring both STMI2 types present => loadware must be transferred twice because the STMI2 firmware can no longer be modified.

  STMI4 boards must have at least the firmware **STMI4_FW_070725** in order to use the optimized load concept for the different CGW-STMI boards.

7.4 Updating Loadware with Web-Based Management

IMPORTANT: Disadvantage
You can only upgrade one IP gateway board at a time.

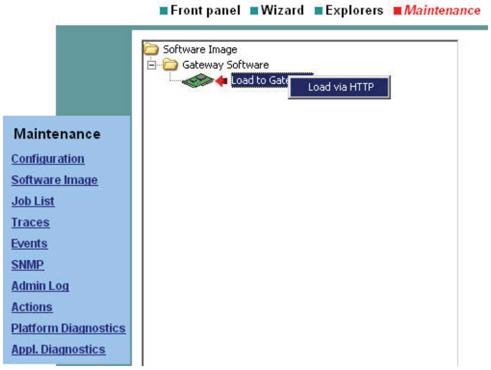
- To use this option, log on to HiPath 4000 Assistant and select **Expert mode > Web-Based Management for HG35xx.**



HG35xx Web Based Management

Board List			
PEN	Board Type	IP Address	Link
1-1-1	STMI2	163.242.210.220	[connect]
1-1-14	STMI2	163.242.210.222	[connect]
1-17-1	STMI2	192.168.6.29	[connect]
1-17-6	NCUI2	163.242.210.215	[connect]
1-18-6	NCUI2+	163.242.210.224	[connect]

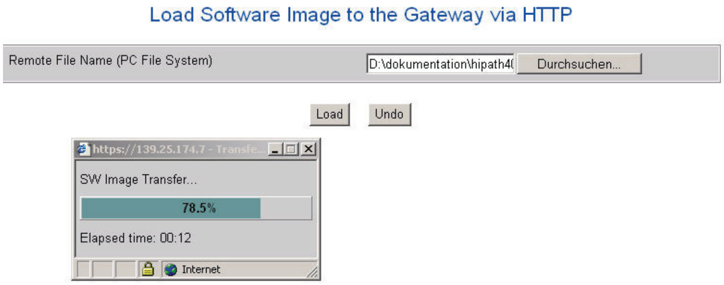
- Now select the required board and click the link **???[connect]**. WBM for HG 35xx now opens.
- Now select **Maintenance > Software Image > Gateway Software > Load to Gateway** and right-click with the mouse.
- Select **Load via HTTP**.



- In the field **Remote File Name (PC File System)** you must enter the software (loadware) saved previously on your PC. This is performed using the **Browse** button.

- Now select the **Load** button to start loading. Loading can take up to five minutes. The loadware is saved in the flash memory of the board.

IMPORTANT: The LAN must be connected but the IP gateway must not be rebooted during the load operation (AMO USSU, AMO BSSU).


Load Software Image to the Gateway via HTTP

Remote File Name (PC File System): D:\dokumentation\hipath4(

SW Image Transfer...

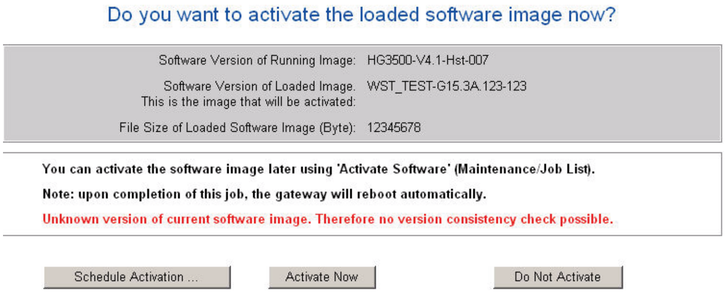
78.5%

Elapsed time: 00:12

- Activate (decompress and install) the loadware.

  Activation (loadware decompression and installation) now takes less than five minutes.

  You can activate the software (loadware) immediately with **Activate Now** or use the **Schedule Activation** button to implement time-controlled activation on a particular day.


Do you want to activate the loaded software image now?

Software Version of Running Image: HG3500-V4.1-Hst-007

Software Version of Loaded Image. This is the image that will be activated: WST_TEST-G15.3A.123-123

File Size of Loaded Software Image (Byte): 12345678

You can activate the software image later using 'Activate Software' (Maintenance/Job List).

Note: upon completion of this job, the gateway will reboot automatically.

Unknown version of current software image. Therefore no version consistency check possible.

7.5 Updating Loadware with "LW Update Manager"

IMPORTANT: Advantage
You can upgrade multiple IP gateway boards at once.

Key features of "LW Update Manager"

- The "LW Update Manager" function lets you upgrade individual boards or all boards supported.
- The LW Update is made up of two parts: Loadware Transfer and Loadware Activation.
- Loadware can be updated immediately or after a delay, that is time-controlled with the scheduler.

Activating "LW Update Manager"

To activate this feature, log on to HiPath 4000 Assistant and select **Expert mode > LW Update Manager**.

For more information, refer to the online help for the "LW Update Manager" or "HiPath 4000 Assistant V4, Loadware Update Manager, Administrator Documentation" on the intranet (http://apps.g-dms.com:8081/techdoc/de/P31003H3440M1450100A9/index.htm).

7.6 General Comments on Loading

Download speed

It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "It takes approximately 8.5 minutes to load a CGW-STMI board (excluding miscellaneous restore times). More time is needed in the case of an access point with a slow IP connection (see also "").Flow control (TCP)").Flow control (TCP)").Flow control (TCP)").Flow control (TCP)").Flow control (TCP)").**Flow control (TCP)**

The system performs flow control. If the necessary bandwidth (quality of service) is not available, the process slows down, that is, the speed is dictated by the slowest access point when loading all access points simultaneously.

8 Save Configuration Data in Local Flash

8.1 Feature Description

Up to HiPath 4000 V4 release 1 backup and restore of HG 35xx WBM configuration is only possible using HiPath 4000 Assistant application „HiPath Backup & Restore“.

There are some customer scenarios, where the gateway boards and HiPath 4000 Assistant are in separated IP-networks (no routing between these two networks) and therefore backup and restore functionality is not possible. In these cases upt o now deault configuration data is used to set up the board again. Then, e.g. trunking connectionns cannot be automatically reestablished. Some furhter data has to be configured.

For example:

- SIP provider connectivity
- Administration LAN and VoIP LAN are separated using firewall

Also in this cases it is required to backup and restore the gateways configuration data.

As of HiPath 4000 V4 release 2 the WBM configurationd ata can be saved in local flash and can be retrieved and used for local backup and restore when connectivity to HiPath 4000 Assistant / backup server is missing.

8.2 Startup Scenarios

Normal restart

Check if the backup server is configured and reachable.

- Backup server is **configured**, **reachable** and **contains a newer version** of configuration data as on the local flash of the board:

  -> Configuration data will be laoded from the backup server. This is normally the case after upgrade over HDLC or exchanging the physical board.

- Backup server is **configured** and **reachable**, but **no backup** with configuration data is stored/found:

  The gateway starts up using its default configuration data. No retry to reach the backup server is executed.

- Backup server is **configured but not reachable**:

A retry to reach the backup server is executed.

- Backup server is **not configured**.

  The gateway starts up using its default configuration data. No retry to reach the backup server is executed.

Loadware Update via HDLC

Same procedures as normal restart. When upgrading via HDLC the board can’t have stored the current configuration data to the local flash (TFFS).

Loadware Update via HiPath 4000 Assistant / WBM

After activating the new loadware the gateway will be automatically rebooted. The new gateway loadware is loaded. The new loadwrae image loads the previously stored configuration data. The data on the backup server can not be more up-to-date, therefore it is not taken into consideration.

For more information on the loadware update via HiPath 4000 Assistant / WBM please refer to Chapter 7, “Load Concept for Gateway Boards”.

Loadware Update via HiPath 4000 Assistant / WBM: backup server not configured

Same as „Loadware Update via HiPath 4000 Assistant / WBM“.

Loadware Update via HiPath 4000 Assistant / WBM: backup server configured but not reachable (via IP)

Same as „Loadware Update via HiPath 4000 Assistant / WBM“.

Loadware Update via HiPath 4000 Assistant / WBM: backup server configured and reachable, but no backup with configuration data is stored/ found

Same as „Loadware Update via HiPath 4000 Assistant / WBM“.

Loadware Update via HiPath 4000 Assistant / WBM: backup server configured and reachable, but on the backup server an older configuration than the current one is found

Same as„Loadware Update via HiPath 4000 Assistant / WBM“.

8.3 Configuration

The feature will be configured with the WBM of the board.

WBM > Maintenance > Actions > (double-click) Automatic Actions > Saving Local Configuration for Upgrade

8.4 Special Use Cases

- Board replacement

  The new board has already a stored backup file in the local flash (but with another functionality than the one that will be replaced).

  Because there is a backup file in the local flash it will be used for restoring the data. But because of the board replacement the MAC address of the board has changed. Therefore HiPath Backup & Restore is contacted to perform a restore with the backup file of the backup server. After the restore from the backup server the correct data is configured on the board. In this case the backup server must be reachable otherwise the board has stored the wrong configuration data.

  After the restore the backup of the local flash should be updated with the current configuration data.

- Default configuration (empty data base)

  An empty data base can be configured as follows:

  WBM > Maintenance > Configuration > (right mouse) **Reset Configuration to Factory Default ...**

  With choosing this option the board will be reseted automatically. During the startup of the board the parameters configured via AMO will be loaded. The WBM parameters will be set to default.

9 Loadability of the FPGA on the STMI4/NCUI4 board

From HiPath 4000 V5 or later it is possible to load the FPGA code on the gateway boards STMI4 and NCUI4.

Usually the FPGA code is supplied with a LW hotfix (or via fix release, minor release, hotfix). There are three files:

- the SENTA file,
- COMGA file for STMI4 and
- COMGA file for NCUI4.

NOTE: The update of the SENTA/COMGA firmware (FPGA code) cannot be done from remote!

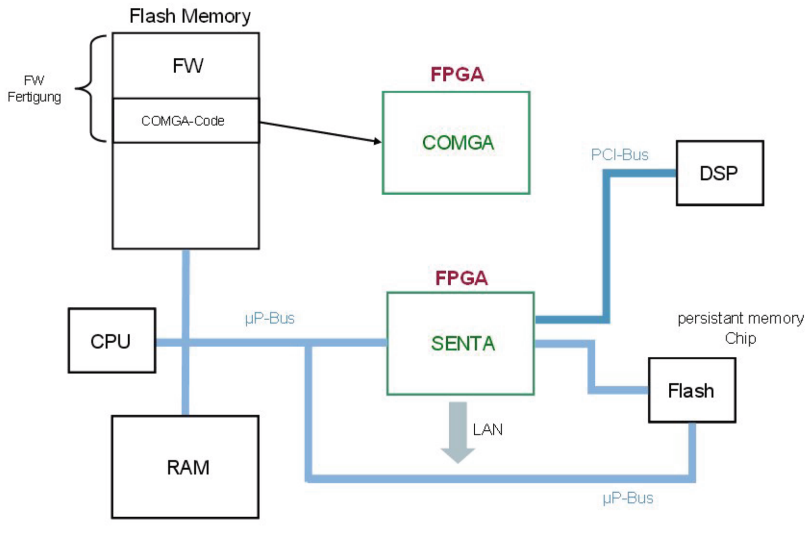


Figure 17 FPGA - Hardware components involved

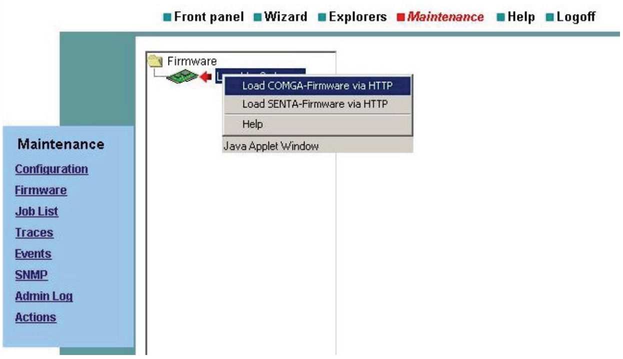
Prerequisite:

The loadware for SENTA /COMGA must be saved via PCHI tool / ftp transfer (**binary**) on the PC. Before the update can be executed, the loadware must be transferred to a PC in the customer’s network and which has access to the WBM of the board (WBM client).

Update:

The update of SENTA loadware and COMGA loadware is done via WBM. In the section **Maintenance > Firmware > Load to Gateway** you have two possibilities:

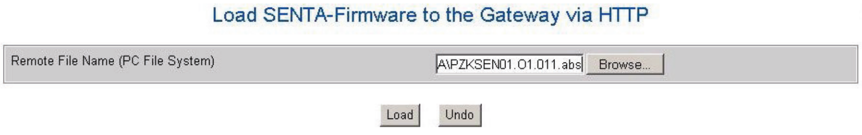
- **Load COMGA-Firmware via HTTP** or
- **Load SENTA-Firmware via HTTP**.



NOTE: The following description of the firmware update is done for SENTA loadware.
For COMGA firmware the instructions are the same but choose **Load COMGA-Firmware via HTTP** from the menu.

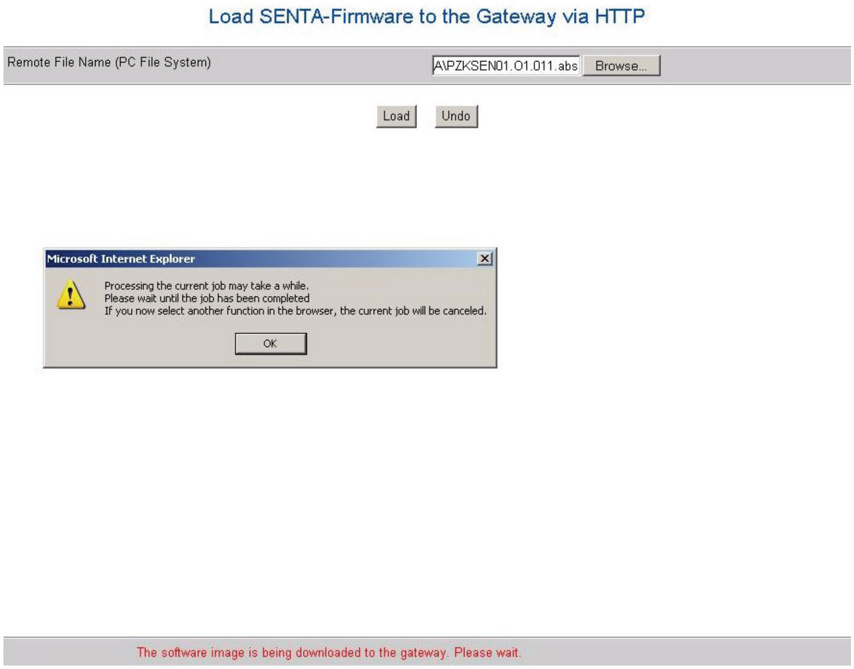
1. Choose **Load SENTA-Firmware via HTTP** from the menu.

1. Select the new file of the SENTA loadware from your local PC by pressing the **Browse** button.


Load SENTA-Firmware to the Gateway via HTTP

Remote File Name (PC File System): A\PZKSEN01.01.011.abs

2. Press the **Load** button for staring the loadware transfer to the flash memeory of the board.



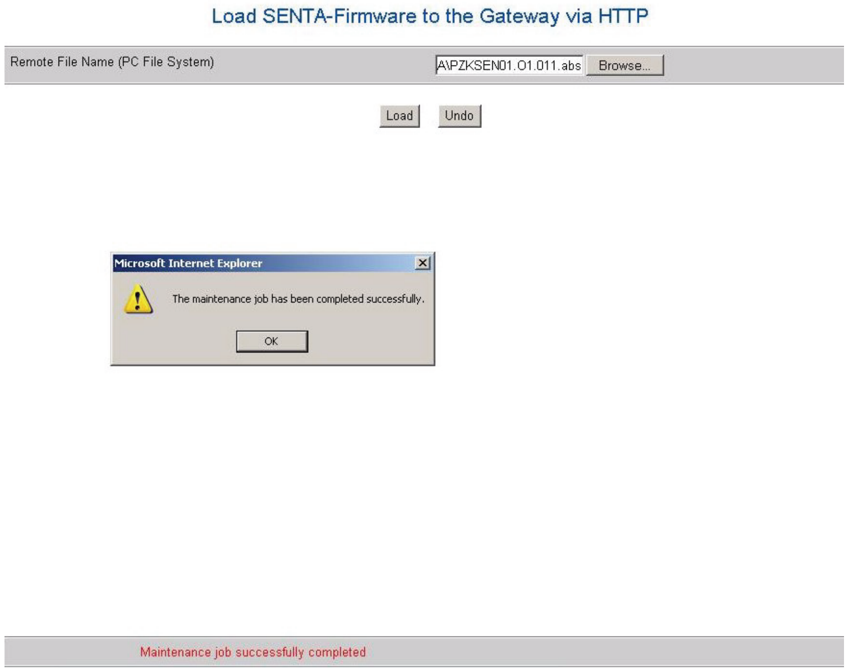
Load SENTA-Firmware to the Gateway via HTTP

Remote File Name (PC File System) A\PZKSEN01.O1.011.abs

Processing the current job may take a while.
Please wait until the job has been completed
If you now select another function in the browser, the current job will be canceled.

The software image is being downloaded to the gateway. Please wait.

3. Upload process has finished when the following screen appears.



Load SENTA-Firmware to the Gateway via HTTP

Remote File Name (PC File System) A\PZKSEN01.O1.011.abs

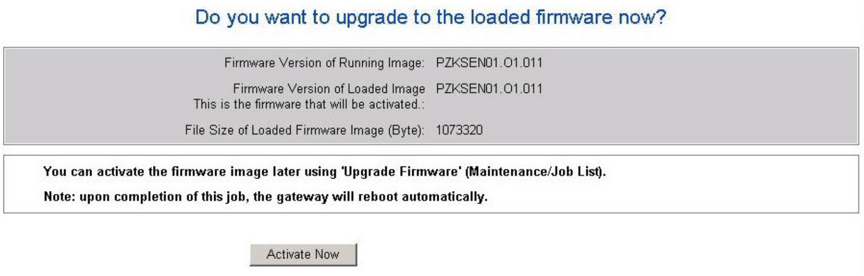
The maintenance job has been completed successfully.

Maintenance job successfully completed

Confirm with **OK**.

4. Activate the new SENTA firmware by pressing the **Activate now** button.

NOTE: After completion of the activation process the gateway will be rebooted automatically!



Do you want to upgrade to the loaded firmware now?

Firmware Version of Running Image: PZKSEN01.01.011

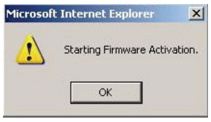
Firmware Version of Loaded Image This is the firmware that will be activated.: PZKSEN01.01.011

File Size of Loaded Firmware Image (Byte): 1073320

You can activate the firmware image later using 'Upgrade Firmware' (Maintenance/Job List).

Note: upon completion of this job, the gateway will reboot automatically.

5. Confirm the activation process by clicking **OK**.



Microsoft Internet Explorer

Starting Firmware Activation.

The new SENTA firmware will be updated, activated and the gateway will be rebooted.

Trace:

The whole process can be monitored with switched on trace SWCONF, level 9 (see **The phase of downloading of the SENTA firmware**).

Failure:

In the case of failure, a popup window appears in the WBM with an error code (see **Traces for failure**). The activation of the loadware and the reboot of the gateway is not performed.

The phase of downloading of the SENTA firmware

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.688177" cswconfigsvc03.cpp 175)
Creating Job! Type=0x1f001b, ID=3

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.701594" cswconfigsvc03.cpp 377)
Created Job 3

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.702931" cswconfjob02.cpp 3357)
Firmware type: SENTA

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.759732" cswconfjob02.cpp 3419)
First block. Retrieving image header.

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.760800" cswconfjob02.cpp 3429)
 offset |  0  1  2  3  4  5  6  7  8   9  a  b  c  d  e  f |
--------+--------------------------------------------------+----------------
00000000| B2 00 00 00 04 30 37 2F  31 30 2F 30 38 31 33 3A | .....07/10/0813:
```

```
00000010| 30 36 3A 35 34 17 45 4C  46 3E 49 33 38 36 50 5A | 06:54.ELF>I386PZ
00000020| 4B 53 45 4E 30 31 2E 4F  31 2E 30 31 32 00 00 00 | KSEN01.O1.012...
00000030| 00 00 30 00 99 78 70 7A  6B 73 65 6E 30 31 00 00 | ..0..xpzksen01..
00000040| 00 00 00 00 00 00 00 00  00 00 00 00 68 00 00 00 | ............h...
00000050| 00 00 00 00 50 D9 10 00  00 00 00 00 00 00 00 00 | ....P...........
00000060| 00 00 00 00 00 00 00 00                          | ........


(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.761791" cswconfjob02.cpp 3652)
Transfer status for job 3 is 1% (11540/1092718)

(SWCONF tBackupTask 0x30622e8 "08/25/2008 15:43:43.774272" cswconfigsvc01.cpp 43
9)
Execute Job in Queue:
    ID = 3, Action=0x1f001b

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.120524" cswconfjob02.cpp 3652)
Transfer status for job 3 is 47% (515348/1092718)

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.497264" cswconfjob02.cpp 3652)
Transfer status for job 3 is 93% (1019156/1092718)

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.590766" cswconfjob02.cpp 3522)
Writing block of 1104096 bytes, remaining 1 bytes

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.465757" cswconfjob02.cpp 3532)
Writing block finished OK.

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.467342" cswconfjob02.cpp 3652)
Transfer status for job 3 is 101% (1104209/1092718)

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474411" cswconfjob02.cpp 3543)
Got last part of the buffer

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474737" cswconfjob02.cpp 3552)
Writing remaining buffer: 0 bytes

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.480742" cswconfjob02.cpp 3614)
 offset |  0  1  2  3  4  5  6  7  8   9  a  b  c  d  e  f |
--------+-------------------------------------------------+-----------------
00000000| 70 7A 6B 73 65 6E 30 31  17 45 4C 46 3E 49 33 38 | pzksen01.ELF>I38
00000010| 36 50 5A 4B 53 45 4E 30  31 2E 4F 31 2E 30 31 32 | 6PZKSEN01.O1.012
00000020| 00 00 00 00 00 30 00 00  00 99 78 30 37 2F 31 30 | .....0....x07/10
00000030| 2F 30 38 20 20 31 33 3A  30 36 3A 35 34          | /08  13:06:54


(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481125" cswconfjob02.cpp 3641)
Writing loadware ID finished OK.

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481718" cswconfjob02.cpp 3652)
Transfer status for job 3 is 101% (1104209/1092718)

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.492219" cswconfigsvc02.cpp 1010)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:51.596658" cswconfigsvc02.cpp 1010)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
```

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:55.651796" cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:57.721041" cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
```

The second phase of the process:

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:22.147227" cswconfjob07.cpp 422)
File info: compressed size: 1104096, uncompressed size: 12491489

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.146807" cswconfjob07.cpp 446)
Uncompression successful

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.147303" util.c 4765)
... writing SENTA FPGA code to SENTA flash

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:33.140242" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:43.140240" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:53.140241" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:03.140241" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:13.140241" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:23.140242" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:33.140478" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:43.140469" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:53.140444" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:03.140352" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:13.140249" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:23.140241" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:33.140242" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:43.140244" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
```

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:53.140248" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:03.140247" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:13.140245" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:23.140242" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:33.140246" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:43.140245" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:53.140244" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:03.140245" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:13.140245" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:23.140245" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:33.140242" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:43.140240" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140243" util.c 4769)
writting SENTA FPGA code to SENTA flash is still running

(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140552" util.c 4771)
programming SENTA flash finished

.....

(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.050407" util.c 3928)
active SENTA version on revision 1: 12

(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.056302" cswconfjob07.cpp 539)
!!! Initializing reboot !!!

(EVTLOG tEvtLogTask 0x36de430 "08/29/2008 10:43:37.058440" cevtlogsvc01.cpp 942)
EventLogEntry from SYSTEM (tEmWeb "08/29/2008 10:43:37.056510" cswconfjob07.cpp
544):
  EventType: Information
  EventCode: MSG_ADMIN_REBOOT
  EventText: Reboot initiated by Admin (Firmware Activation)


Executing Shutdown and Reboot for EvtCode 100 (MSG_ADMIN_REBOOT)

Exiting Security Task*** Shutdown.
```

Traces for failure

```
(SWCONF tFPGAWrite 0x4e39e88 "08/28/2008 15:06:53.579613" util.c
3666)

call of xsvfExecute returned error:2
```

10 Standby Board HG 3500

As of HiPath 4000 V4, this feature is supported for all common gateway boards. Regardless of the boards configuration as single feature mode or as multiple feature support (MFS).

IMPORTANT: Restriction
In the case of MFS, only the entire board can be transferred to the standby board!

10.1 Feature Description

This feature is designed to increase the availability of IP terminals, IP trunking lines, etc, in the event of board failure or LAN cable defects.

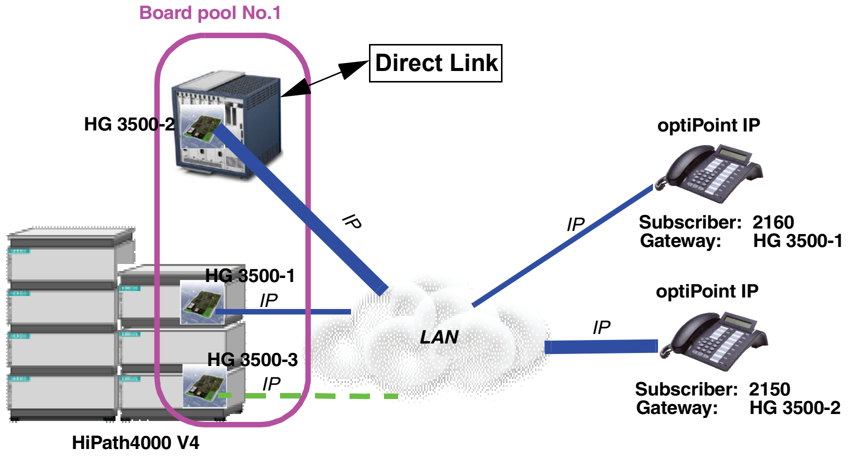


Figure 18 HFA infrastructure

This is achieved through the introduction of a standby board. In the event of a board or LAN cable defect, standby boards can inherit the IP stations or IP trunking lines, etc. assigned to an active board. If appropriately configured, this action can be performed automatically, that is, without manual intervention or use of AMO commands. This is illustrated in the following example which depicts a common gateway with HFA stations.

In the example in Figure 18 HFA infrastructure, the standby board is the HG 3500-3. If, for example, an HG 3500-1 fails, the IP Phone 2160 will be reconfigured to HG 3500-3 and goes into operation with the new board.

Provided this feature was preconfigured (see below), automatic switchover takes place in the following events:

- When the board is removed without prior deactivation

- Faults on the LAN connection cable. Please note that LAN faults that are located “behind“ routers, hubs or IP switches do not trigger a switchover, and nor do faults on IP terminal devices. The switchover mechanism is only triggered by a signaled Layer 1 fault, that is, a general cable defect.
- Faults that are detected by the security system and that lead to the DC status “DEF“ (on board level), for example, “Message not transmittable. Exception: a statistic overflow does not lead to a switchover.

The automatic switchover mechanism is not triggered if either the board or hierarchically superior elements (LTU, LTG) are disabled.

The IP terminals go out of operation during switchover and are automatically put back into operation following a successful switchover. The duration of the switchover process is determined by the board data loading time and by timers on the board and in the terminal device. It normally takes between one and two minutes.

Please note that, following the switchover operation, the board sends a “gratuitous ARP” (Address Resolution Protocol) request to the LAN on startup so that the MAC address (which has changed with the board) associated with the IP address is updated in the LAN components immediately rather than waiting until the aging timer expires. **On the LAN side, take care that the ARP request does not get blocked by any routers that may be involved**.

The automatic switchover is signaled at the service terminal. SYSDEP-NMC also receives a message confirming switchover. Designed specially for this purpos is the NMC alarm 36 (PER-BOARD SWITCHOVER). The message at the service terminal is as follows:

```
F5880 M4 N0542 NO ACT   BPA   BOARD    RECONFIGURATION
06-11-09 10:13:30

    ALARM CLASS:CENTRAL:036

        P101 :LTG1 :LTU3 :055:  0-239:90 Q2316-X10  STMI2/1
BST:01  PLS:-06

     FORMAT:43

      REASON:00H  BOARD RECONFIGURATION OK

      SOURCE BOARD      : P117:LTG1 :LTU17:097:

      DESTINATION BOARD : P101:LTG1 :LTU3 :055:
```

If the service personnel has replaced the defective board on which the IP stations were originally configured with an intact board, then the IP stations can be configured back in the course of manual startup. The board that took over operation after the defect was discovered resumes its role as standby board and is ready for switchover in the event of future defects.

Apart from automatically switching IP stations to a standby board when a defect occurs, this feature also offers manual switchover options that can be implemented with the AMO BSSU. This lets the IP stations maintain their group relationships, which means there is no need for station reconfiguration with the AMO SBCSU, AMO AUN, etc.

The feature must be preconfigured before it can be put into operation. This involves the following steps (for AMO details see Section 10.4, “Generation”):

1. Configure the common gateway board: Both the normal boards (on which the IP stations are configured) and the standby boards are configured as usual with the AMO BFDAT and AMO BCSU. No distinction is made at this stage between the two functions.
2. Configure common gateway board data: The common gateway boards are normally parameterized with the AMO CGWB. The parameters set here determine whether the board will be used as a normal board with IP stations or as a standby board. The normal boards must be assigned an IP address (as in previous configurations), whereas the standby boards are programmed with no IP address or other parameters.
3. All common gateway boards that want to use the feature must be grouped together in a board pool with the AMO BPOOL. A board pool is administered by means of a pool number and must contain both the normal boards and the standby boards. Only when this is complete can a normal board switch over to a standby board in the event of a defect.
   Please note that following a defect, a pool-based board can only be automatically switched to a standby board in the same pool. In the case of AMO-activated manual switchover, on the other hand, the board and standby can be located in separate pools; both boards must, however, belong to a pool (any pool) for this function to work.
4. As usual, the IP stations are configured on the normal boards and put into operation with the AMO SBCSU. Stations cannot be configured on a standby board.

Besides the functionalities described above, the feature also offers the following functions:

- The following attributes can be set on a pool-specific basis:
  – **SINGLE** / **MULTI**

    This setting specifies whether automatic switchover should be performed once (SINGLE) or several times, such as when further defects occur.

  – INFO

    The purpose of this is to provide clarity when operating multiple pools. It may be useful to assign names to pools.
- Trace pool history

A History field is provided for every board in the pool. The following information can be entered here and read out with the AMO BPOOL:

- Board (LTU, slot) from which the stations currently configured were switched
- Board (LTU, slot) to which the stations previously configured were switched
- Date and time at which the IP stations were switched to or from the board
- Counter indicating how often the stations currently configured were switched

This information is available separately for automatic switchover (following a defect) and for manual switchover. The AMO BPOOL can be used to reset the history data (but only for all data simultaneously).

The history only contains information on the last switchover performed. Only the counters provide information on all switchover stages.

IMPORTANT: For automatic IP station switchover to work, the boards must be **in operation** (DC status “Ready“) at the time of the defect. The feature is not implemented if a defect is discovered when starting up the board or the system; in this case, an automatic restart is performed. This is necessary for system stability reasons.
Exception: A detached LAN cable results in a successful start; the later detection of the LAN cable failure activates the automatic switchover as long as a standby board is available.

SINGLE

If **SINGLE** automatic switchover is configured, further defects do not trigger a switchover to a standby board, even if there are standby boards available in the pool. This setting allows stations to be switched back manually after the defective board has been replaced, without having to specify their current location.

MULTI

If **MULTI** automatic switchover is configured, defects continue to trigger switchovers until there are no more standby boards available in the pool. When switching back manually, you must specify the boards from which and to which the stations should be switched. In other words, you must know or find out the source board and the target board.

10.2 User Interface

No particular consequences for telephone users. During the switchover phase, the telephone is “dead“; its display is cleared and reappears as soon as the telephone becomes operational on the new board. Before this point, additional temporary messages such as PBX NOT FOUND may appear on the display.

10.3 Service Information

IP station switchover can be likened to a reconfiguration. This means that reconfiguration does not take effect after a system reload unless the static data was written to the hard disk with `EXEC-UPDAT:BP,ALL;`

IMPORTANT: If a **system reload** is performed after the IP stations have been switched over to a standby board and before backing up the database to the hard disk with the AMO UPDAT, the IP stations remain configured on their old board after the reload. If this old board is still defective or has been removed, **switchover is not performed** because the condition that the board must be in operation at the time of the defect is not satisfied (exception: a defective LAN cable cannot be detected until the board is in operation, and in this case a switchover is performed).

The new type branch to **SMODE** was introduced in the AMO CGWB for this feature.

There are two versions of standby mode:

1. **STBYRDY**: Means “Standby Ready” and describes a standby board that is ready to inherit stations. Normally, the DC status of this board is “Ready” because the board evaluates the standby mode and sends a positive load acknowledgement to the system in response to STBYRDY”. The LAN status can be “Ready” or “DEF”. If a board is to serve as a standby board, both its DC status and the LAN status must be “Ready”.
2. **STBYDEF**: Means “Standby Defect” and describes a board from which the IP stations were switched on account of a defect. This board cannot serve as a standby board because its DC target status is “DEF”. Normally, the DC status of this board is “DEF” or “NL” if the board is inserted or “NPR” if the board is removed. The loadware that evaluates the standby mode sends a negative acknowledgement to the system in response to STBYDEF (DEF ON REQUEST).

Boards that are in standby mode do not have a separate IP address or any board data. The standby board only receives **all the board data** (including the IP address) when they are transferred to it from the source (defective) board on switching over the IP terminals. Following switchover, the source board is transformed into a standby board (for example, STBYDEF), which means it no longer has an IP address. Although the standby board is physically connected to the LAN, meaning that Layer 1 remains in operation, the higher layers are deactivated. **LAN-based access, for example over FTP, Telnet or SNMP, is therefore impossible with a standby board**.

IMPORTANT: Please note that the Ethernet bit rate configured in the board data is also transferred from the source board to the standby board. The LAN segment to which the standby board is connected must therefore have the same bit rate as the source board's LAN segment.

The feature is restricted to a single system: cross-system application is not supported.

It is possible, however, to organize the IPDA architecture in such a way that the common gateway boards and standby boards are randomly distributed over the HHS (HiPath Host System) or in the AP (Access Point). In this case, all boards must be connected to the LAN.

IMPORTANT: It is important to note that LAN-based availability is guaranteed so that not only the active board but also the standby board can reach the IP stations and vice versa.
In addition, be sure to trigger the change in mapping of IP address to MAC address with the previously mentioned ARP requests in the LAN components. This “gratuitous ARP“ request may not be blocked (e.g. in the router configuration).

We recommend testing the automatic switchover mechanism in the course of initial start to ensure it is in working condition and ready to tackle real defects.

As board data is also transferred in the course of manual and automatic station switchover, restrictions apply if the switchover takes place between fully configured (for example, Q2316-X10) and partially configured boards (for example, Q2316-X). Please note the following in this case:

- No restrictions apply if the pool only contains boards of the same type, that is, boards that have the same DSP resources and thus the same number of active connections.
- If you are switching from a partially configured board to a fully configured board, then, following switchover, the number of active connections is restricted to the number supported by the partially configured system. You must increase the UDP port range to be able to use all of the fully configured board's resources. Please note that any existing firewalls must be adapted in line with the new UDP range.

- If you are switching from a fully configured board to a partially configured board, then, following switchover, only a reduced number of active connections is possible on the new board, that is, the number supported by the partially configured board. This can lead to frequent blockages in configurations with many stations and high switching loads.

If manually switching the IP stations from a source board to a target board (command: `RESTART-BSSU:...,CGWSW=SWITCH,...;`), then please note the following points:

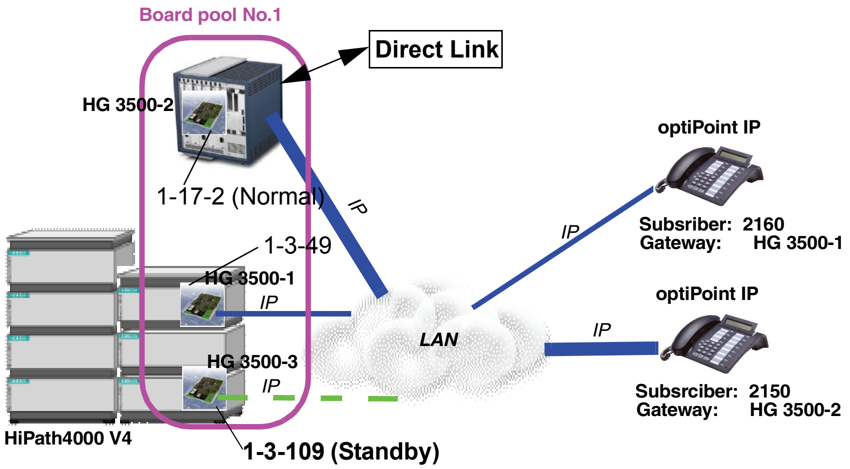
- The target board must be in **STBYRDY** standby mode and its DC status must be “Ready“ (for example, not locked by means of an AMO), and its LAN cable must be connected.
- The source board must not be in standby mode, that is, **SMODE=NORMAL** must be set. Otherwise, the board can display any DC status - it can even be locked by means of an AMO. If this is the case, the manual lock is transferred to the target board. If the DC status or the status of the source board’s LAN connection is “DEF” prior to switchover, **SMODE=STBYDEF** is entered after switchover. In all other cases, **SMODE=STBYRDY** is set, meaning that this board can once again operate as a standby board.

IMPORTANT: To the extent that it plays a role in the switchover, the LAN connection status (Layer 1) can be queried with the AMO BPOOL. And of course you can use the AMO SDSU as before.

SMODE

SMODE describes the common gateway board’s standby mode. Standby mode determines whether a board is configured as a normal board with IP stations, IP address, etc., or whether it is a standby board.

10.4 Generation



In the interest of clarity and to keep things simple, we will not discuss the general configuration of DPLN, LTU, etc. here. However, a list of all common gateway specific commands is provided:

Configure the DIMSU memory for the common gateway boards:

```
   ADD-DIMSU:TYPE=SYSTEM,CGW=4;
```

Configure the common gateway boards:

FCTBLK=1 : HG 3500-1

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3530,BRDBCHL=BCHL60;

CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3530,LINECNT=60,BCHLCNT=30
;

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

FCTBLK=2 : HG 3500-2

```
ADD-BFDAT:FCTBLK=2,FUNCTION=HG3530,BRDBCHL=BCHL120;

CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3530,LINECNT=120,BCHLCNT=6
0;

CHANGE-BFDAT:CONFIG=OK,FCTBLK=2,ANSW=YES;
```

FCTBLK=3 : HG 3500-3 (Reserve-Baugruppe)

```
ADD-BFDAT:FCTBLK=3,FUNCTION=STANDBY,BRDBCHL=BCHL60&BCHL120;
```

Assigning a function block to a board:

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=3,SLOT=49,PARTNO=Q2316-
X,FCTID=1,FCTBLK=1; /*HG 3500-1
```

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=17,SLOT=2,PARTNO=Q2316-
X10,FCTID=1,FCTBLK=2; /*HG 3500-2
```

```
ADD-BCSU:MTYPE=IPGW,LTU=3,SLOT=109,PARTNO=Q2316-
X,FCTID=1,FCTBLK=3; /*Standby board HG 3500-3
```

Configuration of common and global feature board data of the common gateway board. In this example 2 normal and one standby board will be configured:

```
ADD-
CGWB:LTU=3,SLOT=49,SMODE=NORMAL,IPADR=192.16.16.12,NETMASK=255.2
55.255.0; /*HG 3500-1
```

```
ADD-
CGWB:LTU=17,SLOT=2,SMODE=NORMAL,IPADR=192.16.16.10,NETMASK=255.2
55.255.0; /*HG 3500-2
```

ADD-CGWB:LTU=3,SLOT=109,SMODE=STBYRDY; /* Standby board HG 3500-3

Load the board data to the boards:

```
RESTART-BSSU:ADDRTYPE=PEN,LTU=17,SLOT=2,WTIME=10;
```

```
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=109,WTIME=10;
```

```
RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,WTIME=10;
```

Configure a board pool with all boards including standby board(s):

```
ADD-
BPOOL:MTYPE=CGW,LTU=17,SLOT=2,POOLNO=1,HOPAUT=SINGLE,INFO="TEST1
";
```

```
ADD-BPOOL:MTYPE=CGW,LTU=3,SLOT=109,POOLNO=1; /* Standby Board */
```

```
ADD-BPOOL:MTYPE=CGW,LTU=3,SLOT=49,POOLNO=1;
```

Configure the IP stations:

```
ADD-SBCSU:STNO=2150,OPT=OPTI,CONN=IP2,PEN=1-17-2-29,
DVCFIG=OPTIIP,COS1=5,COS2=6,LCOSV1=11,LCOSV2=12,LCOSD1=21,LCOSD2
=22;
```

```
ADD-SBCSU:STNO=2160,OPT=OPTI,CONN=IP2,PEN=1-3-49-0,
DVCFIG=OPTIIP,COS1=5,COS2=6,LCOSV1=11,
LCOSV2=12,LCOSD1=21,LCOSD2=22;
```

Reset FUNSU bit to shorten the Reload time of the STMI2 board

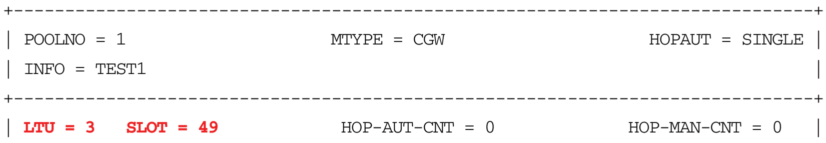
```
CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X",FCTID=3,ACTION=RESET;
```

1. Automatic switchover: This is not controlled by AMO commands but rather is triggered when an active board goes out of service.

   Example prior to automatic switchover:

   ```
   DIS-BPOOL;
   ```

   ```
   H500: AMO BPOOL STARTED
   ```

   ```
   +------------------------------------------------------------------------------+
   | POOLNO = 1                     MTYPE = CGW                   HOPAUT = SINGLE |
   | INFO = TEST1                                                                 |
   +------------------------------------------------------------------------------+
   | LTU = 3   SLOT = 49           HOP-AUT-CNT = 0              HOP-MAN-CNT = 0   |
   ```

```
| DC-STATUS = READY              LAN_VERB = READY            SMODE = NORMAL      |
+------------------------------------------------------------------------------+
| LTU = 3    SLOT = 109           HOP-AUT-CNT = 0              HOP-MAN-CNT = 0   |
| DC-STATUS = READY              LAN_VERB = READY            SMODE = STBYRDY     |
+------------------------------------------------------------------------------+
| LTU = 17   SLOT = 2             HOP-AUT-CNT = 0              HOP-MAN-CNT = 0   |
| DC-STATUS = READY              LAN_VERB = READY            SMODE = NORMAL      |
+------------------------------------------------------------------------------+
```

If board 1-3-49 now becomes defective, all board data and all IP stations are switched to standby board 1-3-109. This provides the following AMO BPOOL output after the switchover:

```
DIS-BPOOL;
H500: AMO BPOOL STARTED
```

```
+------------------------------------------------------------------------------+
| POOLNO = 1                     MTYPE = CGW                    HOPAUT = SINGLE |
| INFO = TEST1                                                                 |
+------------------------------------------------------------------------------+
| LTU = 3     SLOT = 49           HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = NPR                LAN_VERB =                  SMODE = STBYDEF     |
| SWITCHED AUTTO BRD LTU = 3       SLOT = 109      DATE/TIME : 2003-09-25 18:07 |
+------------------------------------------------------------------------------+
| LTU = 3     SLOT = 109          HOP-AUT-CNT = 1             HOP-MAN-CNT = 0    |
| DC-STATUS = READY              LAN_VERB = READY            SMODE = NORMAL      |
| SWITCHED AUTFR BRD LTU = 3       SLOT = 49       DATE/TIME : 2003-09-25 18:07 |
+------------------------------------------------------------------------------+
| LTU = 17    SLOT = 2            HOP-AUT-CNT = 0             HOP-MAN-CNT = 0    |
| DC-STATUS = READY              LAN_VERB = READY            SMODE = NORMAL      |
+------------------------------------------------------------------------------+
```

Explanation of important abbreviations in the output:

HOPAUT: Automatic switchover between the boards in this pool is permitted once (SINGLE) or several times (MULTI).

SMODE: Standby mode (see Section 10.3, “Service Information”)

HOP-AUT-CNT: Number of automatic switchovers

HOP-MAN-CNT: Number of manual switchovers

DC-STATUS: The board’s DC status (see also AMO SDSU)

LAN_VERB: LAN connection status; READY generally means “LAN cable connected”, DEF means “LAN cable disconnected or defective”. If the field is empty, the LAN connection has a DC status which does not get interpreted by the AMO BPOOL. In this case, the LAN status has no effect on switchover. If this is of interest, you can use the AMO SDSU.

The following history data is only displayed after a switchover:

SWITCHED AUTFR BRD: The IP stations were automatically switched away from this board (for example, on account of a defect) (see also **DATE/TIME**)

SWITCHED AUTTO BRD: The IP stations were automatically switched back to this board (for example, on account of a defect in another board) (see also **DATE/TIME**)

SWITCHED MANFR BRD: The IP stations were manually switched away from this board (with the AMO BSSU) (see also **DATE/TIME**)

SWITCHED MANTO BRD: The IP stations were manually switched back to this board (with the AMO BSSU) (see also **DATE/TIME**)

The history data can be reset with the following AMO command:

```
CHANGE-BPOOL:MTYPE=CGW,TYPE=HISTRES,LTU=3,SLOT=109;
```

All functions assigned to board 1-3-49 are now transferred to board 1-3-109, including the board's IP address and all IP stations. The supplementary information shows the history of the last switching operation. This example shows that on 25.9.2003, a switchover occurred from 1-3-49 to 1-3-103 because board 1-3-49 was removed (DC status NPR).

The counters HOP-AUT-CNT and HOP-MAN-CNT are set for boards with SMODE=NORMAL. All history data is deleted for standby boards.

2. Manual switchover with the AMO BSSU:

   a) The stations switched away from 1-3-49 on account of a board defect should be switched back into service following the repair of 1-3-49:

   ```
   RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=IPSTNBCK;
   ```

   or

   ```
   ACTIVATE-BSSU:LTU=3,SLOT=49,CGWSW=IPSTNBCK;
   ```

   b) All IP stations assigned to board 1-3-49 should be switched to standby board 1-3-109:

   ```
   RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=SWITCH,
   LTU2=3,SLOT2=109;
   ```

   Please note that any AMO lock set will be transferred to the target board (see also Section 10.3, "Service Information")

   c) A board that is in **STBYDEF** standby mode because of a defect, for example, and because the IP stations were switched away should resume its standby board role. This generally occurs after it has been repaired or the board has been replaced. The following command can be used for this:

   ```
   RESTART-BSSU:ADDRTYPE=PEN,LTU=3,SLOT=49,CGWSW=STBYRDY;
   ```

3. Shorten the Reload time of the common gateway board

   ```
   CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X",FCTID=1,ACTION=RESET;
   ```

10.5 Service steps after the automatic switch over

Two steps can be different after a switch over in case of error:

1. The subscribers which are switched over should get their original pens.

   In this case the board pool has to be defined as **HOPAUT=SINGLE** !

   – Change the defective board resp. reconnect the LAN connection.

   – Switch back the subscribers with the AMO command

     ```
     RESTART-BSSU:ADDRTYPE=PEN,LTU=xx,SLOT=xx,CGWSW=CGWSWBCK;
     ```
     (xx -> Pen of the board with status **STDBYDEF**)

   – Reset the history data of the Board Pool:

     ```
     CHANGE-BPOOL:MTYPE=CGW,TYPE=HISTRES,LTU=y,SLOT=zz;
     ```

2. The subscribers which are switched over should remain on the new pens.

   In this case the board pool has to be defined as **HOPAUT=MULTI** !

   – Change the defective board resp. reconnect the LAN connection.

   – Switch the STDBYDEF board to **STDBYRDY** with the AMO command

     ```
     RESTART-BSSU:ADDRTYPE=PEN,LTU=xx,SLOT=xx,CGWSW=STBYRDY;
     ```

10.6 Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanaele fuer die HG3530 Funktion
	BCHL3530	e	Number of b-channels for HG3530 function
	FCTID	d	Function Id (muss immer 1 sein)
	FCTID	e	Function id (must always be set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Index to loadware block for the t1 board
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	ontinue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway 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 eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 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.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	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.

BPOOL	ART	d	Art der Pool-Daten:
			ALLE = Alle Pools löschen
			ATTR = Pool-Attribut ändern
			BAUGR = Baugruppe aus Pool löschen
			HISTRES = Historie der Baugruppe rücksetzen
			POOL = Einen bestimmten Pool löschen

	TYPE	e	Type of pool data: ALL = Delete all Pools ATTR = Change pool attribute BOARD = Delete board from pool HISTRES = Reset history for a board POOL = Delete a specific pool
	EBT	d	Einbauteilung
	SLOT	e	Slot

	HOPAUT	d	Pool-Attribut für die Hop-Kontrolle beim automatischen Umschalten:
			SINGLE = nur automatisches einmaliges Umschalten erlaubt
			MULTI = mehrfaches automatisches Umschalten erlaubt

	HOPAUT	e	Pool attribute for the hop control for automatic switchover: SINGLE = Automatic switchover is allowed only once MULTI = Automatic switchover is allowed several times
	INFO	d	Pool-Attribut: Informationstext
	INFO	e	Pool attribute: Information text
	LTU	d	Line Trunk Unit
	LTU	e	Line Trunk Unit
	MTYP	d	Modultyp, derzeit nur CGW möglich
	MTYPE	e	Module Type, currently onl CGW possible
	POOLNR	d	Nummer des Baugruppen-Rekonfigurations-Pools
	POOLNO	e	Number of the Board Reconfiguration Pool

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BSSU	CGWSA	d	CGW Schaltauftrag: CGWSWBCK: Rückschalten aller automatisch weggeschalteter IP Teilnehmer auf die Original-CGW-Baugruppe KEIN: Kein CGW bezogener Schaltauftrag STBYRDY: Verwendung als CGW Standby-Baugruppe (Reserve-Baugruppe) UMSCH: Umschalten der IP Teilnehmer der CGW-Baugruppe auf eine andere Baugruppe
	CGWSW	e	CGW switching activity: CGWSWBCK: Switch IP stations back to original CGW board NONE: No CGW specific activities STBYRDY: Act as CGW standby board SWITCH: Switchover IP stations of CGW board to another board
	LTG2	d	Line Trunk Group der Zielbaugruppe bei CGWSA=UMSCH
	LTG2	e	Line Trunk Group of the destination board of CGWSW=SWITCH
	LTU2	d	Line Trunk Unit der Zielbaugruppe bei CGWSA=UMSCH
	LTU2	e	Line Trunk Unit of the destination board of CGWSW=SWITCH
	EBT2	d	Einbauteilung der Zielbaugruppe bei CGWSA=UMSCH
	SLOT2	e	Slot of the destination board of CGWSW=SWITCH
CGWB	SMODE	d	Standby Mode oder Normal Mode **Normal**: Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. **STDBYRDY**: Eine Baugruppe im Standby Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. **STDBYDEF**: Eine Baugruppe im Standby Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SMODE	e	Standby Mode or Normal Mode **NORMAL**: A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. **STDBYRDY**: A board in Standby Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. **STDBYDEF**: A board in Standby Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network addresss part but different host address parts (also the Default Router must fulfill this requirement)
FUNSU	AKTION	d	Ladeart der Baugruppe: Damit der LW Code nicht bei jedem Baugruppen-Reset geladen wird, sollte RESET eingestellt sein.
	ACTION	e	Action set or reset loadware on board: In order to avoid loading of the LW code, it is recommended to set this parameter to RESET.

11 DLS Client Bootstrapping

DLS client bootstrapping is a procedure that must be performed once to allow the DLS server to exchange configuration data with the gateway. This procedure generates an individual (DLS) certificate for the gateway and transfers it to the gateway. The gateway and DLS can then use these certificates for unique reciprocal authentication.

11.1 Bootstrapping with "No PIN" PIN Mode

Variant A:

1. Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration**.
2. Contact the gateway in DLS via **IP Devices > IP Device Interaction > Scan IP Devices**. Enter **8084** in the Port field in the **"IP Ranges"** tab.

If everything is in order, the value **Secure** appears in the **Security Status:** field in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab.

Variant B:

1. Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration**.
2. Enter the IP address of the DLS server at the gateway with the CLI command `set dls ip_address`. The port is usually 18443.
3. Enter the CLI command `contact DLS` at the gateway.

11.2 Bootstrapping with "Default PIN" or "Individual PIN" PIN Mode

Variant A:

1. Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab and then select the required PIN mode.
2. Contact the gateway in DLS via **IP Devices > IP Device Interaction > Scan IP Devices**. Enter **8084** in the Port field in the **"IP Ranges" tab**.
3. Enter the CLI command `activate dls pin <pin>` at the gateway with the PIN displayed under 1.

Variant B:

1. Create a virtual IP device in the DLS under **IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"** tab and then select the required PIN mode.
2. Enter the IP address of the DLS server at the gateway with the CLI command `set dls ip_address`. The port is usually 18443.
3. Enter the CLI command `contact DLS` at the gateway.
4. Enter the CLI command `activate dls pin <pin>` at the gateway with the PIN displayed under 1.

12 HiPath Gateway HG 3575 V4 - Changing Parameters with AMO STMIB

IMPORTANT: Any of the settings that can be made here with AMOs are read-only in WBM.

The following branches are supported:

- TYPE GLOBAL - Changing the Idle Bit Pattern
- TYPE IFDATA - Changing the Interface-Specific Parameters of the Access Point
- TYPE SERVIF - Changing the Login and Password for Service Access
- TYPE ASC - Changing the Payload QoS Setting of the Access Point
- TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activity Detection and T.38 Fax
- TYPE DSP - Jitter Buffer Size of the Access Point
- TYPE DMCDATA - Changing the Access Point Setting to Support Direct Media Connections
- TYPE H323 - Changing the H323 Settings at the Access Point
- TYPE JB - Configuring the Jitter Buffer
- TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP
- TYPE SNMP - Changing the Community Strings for Read Access
- TYPE WBMDATA - Changing the Login and Password for WBM
- TYPE GWSECTOR - Changing the Access Point Sector Number for the Resource Manager
- TYPE DLSDATA - Configuring DLS Data
- Resetting the Parameters to Default Values

12.1 TYPE GLOBAL - Changing the Idle Bit Pattern

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter idle bit pattern on the **General** tab and **Save**.

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,SLOT=99,TYPE=GLOBAL,PATTERN=2
13;
```

This change does not become effective until the access point is 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=99;
```

IMPORTANT: Connections are cleared down without further warning.
Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

12.2 TYPE IFDATA - Changing the Interface-Specific Parameters of the Access Point

The settings can differ from access point to access point.

The following parameters can be set:

- For the physical Ethernet interface [`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) [`TOSLAN, TOSMODEM`]

The Ethernet interface setting **must** be **identical** for both connected interface partners (HG 3575 or LAN switches, routers).

IMPORTANT: The setting of a fixed interface partner leads to problems with the “Autonegotiate“ setting of the other partner.
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 connected to the HG 3575 does not support autonegotiation or if it does not work reliably, fixed values must be set for the HG 3575’s Ethernet interface.

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”. According to the standard, the VLAN ID must then be set to zero, which also happens for the default setting.

In the example, VLAN tagging is deactivated (reset to the default value), the standard TOS values are configured without DiffServ (see Table 2, “TOS values”) and the Ethernet interface is set to 10 Mbps half duplex.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the TOS bytes under Layer 2 and Layer 3 on the **Quality of Service** tab.
Set the transmission speed and mode on the **Ethernet Interface** tab and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=IFDATA,VLAN=NO,
TOSLAN=20,TOSMODEM=16,BITRATE=100MBFD;
```

This change does not become effective until the access point is 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=99;
```

IMPORTANT: Connections are cleared down without further warning.
Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

12.3 TYPE SERVIF - Changing the Login and Password for Service Access

The HiPath HG 3575 allows the connection of a TAP/Service PC via RS232/V.24 interface.

There are two operating modes:

- Terminal Mode

  In terminal mode, communication with the HiPath HG 3575 Loadware is realized directly via the Command Line Interface.

  IMPORTANT: HiPath 4000 V4 or higher does not support two-stage CLI.

  ```
  CHANGE-
  STMIB:MTYPE=NCUI2,LTU=<LTU>,SLOT=<SLOT>,TYPE=SERVIF,LOGINT
  RM=<User login for terminal mode>,LOGINPPP=<User login for
  PPP connection>,PASSW=<Password for terminal mode>;
  ```

  The standard login data is:

  Login: TRM (parameter (**LOGINTRM**)

  Password: PUBLIC (parameter **PASSW**)

  After successful login the following message appears:

  ```
  Welcome to the HG 3575 V4.0 <LW-version> Command Line
  Interpreter.

  vxTarget>
  ```

  A list of available commands can be now requested via the local help function which is available via the `help` command.

- PPP Mode

  In PPP mode, a link between the TAP/Service PC and the customer network is established via the HiPath HG 3575 using the IP address configured with the AMO APRT, parameter **TAIPADDR**.

  Login (default setting): PPP

  Password: No password is required for PPP!

  IMPORTANT: For security reasons, the configured password cannot be exported or regenerated.
  The passwords are therefore deleted when a system is regenerated from the REGEN batch.
  Logins and passwords set in the system are always stored in uppercase.

These 3 parameters can be configured differently per module.

In the example, the login for AP 17 is set to TERMINAL and SURV, while the password is set to HG3575:

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the user data on the **Security** tab and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=17,TYPE=SERVIF,

LOGINTRM=TERMINAL,LOGINPPP=SURV,PASSW2=HG3575;
```

This change does not become effective until the access point is 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=17;
```

IMPORTANT: Connections are cleared down without further warning.
Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

<LW-version>

<LW-version> holds the currently loaded loadware version number (e.g. L0-TOS.10.030-004)

12.4 TYPE ASC - Changing the Payload QoS Setting of the Access Point

In this branch, the Quality of Service for the payload of an access point can be configured. The settings can differ from access point to access point. If the routers do not support DiffServ, the standard TOS value must be configured without DiffServ. If DiffServ is supported, but not the Siemens CodePoints, the value specified by the network operator must be configured.

In the example, the standard TOS value is set for AP 99 without DiffServ (see also Table 2, “TOS values”).

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the TOS bytes under Layer 3-Diffserv on the **Quality of Service** tab and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,TOSPL=16;
```

This change is started directly on the access point and is effective immediately without an interruption in operation.

12.5 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activity Detection and T.38 Fax

See also Chapter 15, “Codec Settings”.

Codec list

With NCUI2, direct media connections from IP phones, trunking gateways or HG 3500/75 gateways associated with networked HiPath 4000 systems can be terminated on the board. Unlike for IPDA, the codec type for DMC connections is not selected using classmarks but rather on the basis of a codec list which provides the relevant partners with information about the codec types supported and preferred.

HG 3575 supports two codec types: G.711 and G.729

The sequence in which the codec types are named defines the preference. The type named first is preferred.

In the example, NCUI2 supports G.711 and G.729 but G.729 is preferred. The audio sample size for G.711 and G.729A is set to 60 ms.

T.38 Fax

The parameter **T38FAX** cannot be used at the moment because this feature is not yet supported on NCUI.

The dafault value has been set to **NO** and cannot be changed to **YES**. The AMO shows up a **warning** when trying to change the value to **YES**.

warning

```
H35: THE T38FAX IS NOT YET SUPPORTED ON NCUI BOARDS,
THE DEFAULT VALUE HAS BEEN SET INTERNALLY.
```

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Select **G729**, **G711** on the **General** tab under **DMC Codec List** in the **Direct Media Connection** section and **Save**.

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,PRIO=PRIO1,CODEC=G72
9,RTP=60;

CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,TYPE=ASC,PRIO=PRIO2,CODEC=G71
1,RTP=60;
```

This change is started directly on the access point and is effective immediately without an interruption in operation.

12.6 TYPE DSP - Jitter Buffer Size of the Access Point

The parameter JITBUFD only takes effect if the parameter JBMODE in the JB branch is set to 0 (LEGACY MODE). JBMODE=0 (=LEGACY MODE) is no longer supported as of HiPath 4000 V4. The jitter buffer size therefore no longer needs to be set.

The parameters of this branch only apply to one access point. Therefore, every access point could be configured differently at a HiPath 4000 switch.

However, in order to maintain the ease of use and the diagnostic capability of the system, these parameters must be configured identically for all access points and HiPath HG 3500s!

In the example, the jitter buffer for AP 17 is set to 100 ms.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the values on the **General** tab under **CODEC Settings** and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,
LTU=17,TYPE=DSP,JITBUFD=100;
```

These changes are started directly on the access point and become effective immediately without interrupting operation.

12.7 TYPE DMCDATA - Changing the Access Point Setting to Support Direct Media Connections

This parameter is used to set if or how many direct media connections are permitted simultaneously on a specific HG 3575. The connections are counted both in the HiPath 4000 central system’s software and on the board itself.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter under **Direct Media Connection (DMC) enabled** on the **General** tab and **Save**.

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,TYPE=DMCDATA,DMCALLWD=YES,DMC
CONN=30;
```

This change does not become effective until the access point is 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=99;
```

IMPORTANT: Connections are cleared down without further warning.
Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

12.8 TYPE H323 - Changing the H323 Settings at the Access Point

Direct media connections use the H323 fast connect mechanism to set up connections. The NCUI2/4 and STMI2/4 platform consequently supports H.323. Two timers from the H.323 stack and the gateway name can be modified.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter under **Direct Media Connection (DMC) enabled** on the **General** tab and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=H323,Q931T1=50,
        Q931T2=500,GWNAME=“HG3575-2“;
```

This change is started directly on the access point and is effective immediately with the next H.323.

12.9 TYPE JB - Configuring the Jitter Buffer

As of HiPath 4000 V4, only the adaptive jitter buffer (JBMODE=2) and the static jitter buffer (JBMODE=1) are supported in the HG 3575 V4 gateway. If JBMODE=0 (LEGACY MODE) is set in the AMO STMIB, this is mapped to the static jitter buffer (JBMODE=1) in the gateway.

A basic understanding of procedures and configuration parameters is required to perform configuration. Refer to Section 2.5, “Jitter Buffer”.

The adaptive jitter buffer (JBMODE=2) that reduces delays is set by default.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the parameter on the **General** tab under **Jitter Buffer** and click **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=JB,

AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4,
               AVGDLYD=60,MAXDLYD=200,JBMODE=2;
```

These changes are started directly on the access point and become effective when the next connection is set up.

12.10 TYPE SIGQOS - Quality Monitoring for the Signaling Connection over IP

Generation

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

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SIGQOS,
              BANDW=40,MAXRTD=500,MINTHRPT=30,
              SIGPTHSW=EXTENDED,QOSSTAT=NO;
```

The setting becomes effective immediately.

12.11 TYPE SNMP - Changing the Community Strings for Read Access

The HG 3575 board operates an SNMP agent that can be address over LAN. You can disable SNMP access completely with the parameter FACCMODE in the DEBUG branch of the AMO STMIB (FACCMODE=2).

HG 3575’s SNMP agent exclusively supports read-only access.

Access authorization and access rights are controlled by the SNMP agent over community strings.

A MIB browser that sends queries to the SNMP agent, identifies itself as belonging to a community. The community is identified by a community string. This is a simple, unencrypted text.

The standard setting - and default for community string 1 (CS1) - is “public“, CS2 is not used.

These values can be modified. CS2 can be used to assign read-only access to a second community on the SNMP agent.

If, for example, CS1="ToP_SeCrEt23" is set and CS2="11!$ZwY?", access attempts using all other community strings (including "public") are rejected.

For the parameters CS1 and CS2, all ASCII characters between «!» (exclamation mark, 33 Dec) and «~» (tilde, 126 Dec) are used with the exception of the characters «"» (34 Dec), «/» (47 Dec), «\» (92 Dec), and «^» (94 Dec). The space character « » (32 Dec) may not be used.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter on the **Security** tab under **SNMP** and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SNMP,
CS1=‟ToP_SeCrEt23‟,CS2=‟11!$ZwY?‟;
```

This change does not become effective until the access point is 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**.

```
DEACTIVATE-USSU:LTG=1,LTU=99;

ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=99;
```

IMPORTANT: Connections are cleared down without further warning.

CS1 cannot be deleted. The following procedure is recommended for deleting CS2:

- Reset all parameters in the SNMP AMO branch to the default value (CS1="public", CS2 inactive)

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

  ```
  CHANGE-STMIB:MTYPE=INITNCU2,LTU=99,TYPE=SNMP;
  ```

- Restore the required values for CS1

  Configuration Management --> System Data --> IPDA --> IPDA Access Point
  Click **Search** and select the access point.
  Enter on the **Security** tab under **SNMP** and **Save**.

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=SNMP,
CS1=“ToP_SeCrEt23“;
```

- This change does not become effective until the access point is 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**.

```
DEACTIVATE-USSU:LTG=1,LTU=99;
ACTIVATE-USSU:UNIT=LTG,LTG=1,LTU=99;
```

IMPORTANT: Connections are cleared down without further warning.

12.12 TYPE WBMDATA - Changing the Login and Password for WBM

WBM access can be configured in this branch.

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=<LTU>,SLOT=<SLOT>,TYPE=WBMDATA,LOGINWBM
=<User login for WBM connection>,PASSWWBM=<Password for WBM
connection>,ROLE=<Role of the WBM user; sets access rights>;
```

Role	Rights
ADMIN	Administrator (default value)
ENGR	Developer (access to all features)
READONLY	Administrator with read-only access
SU	Superuser (access to all features)

Table 18 WBM rights

The data for initial login as ENGR is:

User name: `HP4K-DEVEL`

Password: `Siemens2000`

12.13 TYPE GWSECTOR - Changing the Access Point Sector Number for the Resource Manager

In this branch, the parameter GWSECTNO is used to assign the HG 3575 gateway a sector number from the Resource Manager’s sector concept.

Details on the Resource Manager’s sector concept and bandwidth management for gateways can be found in the Resource Manager Service Manual (Complex Solutions, under the “Large Enterprise Gatekeeper” feature).

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the **Gateway Sector Number** on the **General** tab and click **Save**.

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=99,TYPE=GWSECTOR,GWSECTNO=7;
```

This change becomes effective immediately and without interrupting operation.

12.14 TYPE DLSDATA - Configuring DLS Data

```
CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=DLSDATA,DLSIPADR=<number>,
DLSPORT=<number>,DLSACPAS=<param>;
```

12.15 Resetting the Parameters to Default Values

If the parameters of one or all branches of the NCUI2/4 data are to be reset to default values, e.g. after being changed temporarily for diagnostic work, this can be performed in the INITNCU2 branch. The example sets all ASC parameters to their default values.

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

```
CHANGE-STMIB:MTYPE=INITNCU2,LTU=17,TYPE=ASC;
```

The changes under TYPE ASC, DSP, H323, JB, SNMP, MGNTDATA, WBMDATA and DLSDATA **become effective immediately** without interrupting operation.

Changes under TYPE GLOBAL, IFDATA, SERVIF, DMCDATA and SIGQOS **become effective after the access point has been restarted**.

This behaviour is also valid for the command `CHANGE-STMIB:MTYPE=INITNCU2,LTU=17,` **`TYPE=ALL`**`;`. Therefore it is recommended to restart the access point after resetting all parameters.

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=17;
```

IMPORTANT: Connections are cleared down without further warning.
Prior to the `EXEC-USSU:UPDATAP`, the configuration must be updated on the system hard disk.

---

13 General Information on How to Configure a HG 3500 V4 Common Gateway

13.1 Changing the common gateway configuration

Please note that the entire board must be reconfigured if changes are made to the common gateway configuration.

13.2 AMOs

- The STMI boards are configured in HiPath 4000 V3.0 using the AMO HFAB and the AMO STMIB. This is done in HiPath 4000 V4 or higher with the AMO CGWB or, if the IPDA was set, with the AMO BCSU (see Chapter 16, “Multiple Feature Support Configuration at the Common Gateway (Example)”).
- The NCUI board is still configured with the AMO STMIB.
- The AMO BFDAT for block configuration is new in HiPath 4000 V4.
- Functions are consolidated on a single board using the AMO BCSU.
- The DB line range of a board must be consecutive.
- All HG 3500 modules must be connected at the HiPath 4000 LAN segment.
- The lines configured for a board cannot be subsequently modified. The entire board must be reconfigured if additional lines are required on a board.
- The parameter FCTID in the AMO BCSU must always be set to 1 in HiPath 4000 V4 and higher. In HiPath 4000 V3.0 and earlier versions, this parameter is used to determine the function of the STMI board (HFA, IPDA, trunking, etc.). In HiPath 4000 V4 (and later), this is defined with the AMO BFDAT.

13.3 Rules

- The parameter for the functional block (**FCTBLK**) can be freely assigned. It may not, however, remain unassigned.
- A completed (configured) functional block may be assigned to one or more boards.
- The parameter for the boards to be used (**BRDBCHL**) determines how many B channels are available to the board.

If the value **BCHAN60&BCHAN120** is set, an STMI[1] with 60 or 120 B channels can be used. This value is also useful if a small STMI with 60 B channels becomes defective. This can then be replaced with a large STMI with 120 B channels. It is not possible to replace a large STMI with a small one.

- Parameter **UNITS**
  - 1 unit corresponds to 10 B channels
  - If the number of units (**UNITS**) is not specified for the configuration, 10 B channels (**UNITS=1**) are configured for each circuit.
  - Up to three units can be specified for each circuit.
  - The total number of B channels for the function is calculated by multiplying the number of circuits (**LINECNT**) by the number of B channels in a unit (**UNITS**).
    Example: LINECNT=4, UNITS=3. 4 multiplied by 3 multiplied by 10 equals 120 B channels.
- If an IPDA function (HG3570) is to be configured for a multiple feature configuration, this must be configured first.
- For **IPDA**, only the number of B channels (**BCHLCNT**) must be specified.
- For **IP trunking**, the number of circuits (**LINECNT**) and the number of units (**UNITS**) must be specified.
- For **HFA** and **SIP**, the number of circuits (**LINECNT**) and the number of B channels (**BCHLCNT**) must be specified.

> If reserved HFA or SIP circuits are to be configured, the B channels designated for this purpose must also be specified here.
> This is not necessary for reserved trunk circuits as the assignment is performed based on the number of units (**UNITS**).

- For **WAML**, only the number of units (**UNITS**) must be specified.

> Only one circuit is possible for WAML.
> This parameter can be omitted if **UNITS=1**.

- **Reserve function**

[1] STMI stands for STMI2 (Q2316-X, Q2316-X10) and STMI4 (Q2324-X500,Q2324-X510)

Since the board configuration can only be modified by removing the board, an option has been created that allows users to reserve circuits for use at a later stage. If this feature is to be used for the functions HG3530, HG3540 or HG3550, the relevant function must be configured directly after the actual function (HG3550&HG3550R, for instance). The Reserve function must always be specified after the actual function (i.e. at the end).

The combination HG3550&HG3530&HG3550R is not permitted as this would lead to invalid circuit distribution (Trunk - HFA - Trunk).

It is not possible to configure several Reserve functions on a single board.

The reserved circuits can be subsequently converted to usable circuits with

```
CHANGE-BCSU:TYPE=IPGW,LTU=<LTU>,SLOT=<slot>,CHNGRSLN=<number>;
```

```
/*<number>: Number of circuits that should be converted to usable
circuits.
```

> Now you must reset the board.
> `RESET-BSSU:ADDRTYPE=PEN,LTU=<ltu>,SLOT=<slot>;`

- The **STANDBY** function can only be configured as a single feature.
- Eleven single-feature standard profiles are configured in the database (see AMO description, AMO BFDAT).
- You can configure a functional block with

  CHANGE-BFDAT:**CONFIG=OK**,FCTBLK=<number>,**ANSW=YES**;

  You can check the status with `DISPLAY-BFDAT:FCTBLK=<number>;`

  If the configuration of the functional block is complete **STATUS=OK** is displayed.

  If a configuration error is detected when the block configuration is complete, the functional block must be deleted (`DELETE-BFDAT:FCTBLK=<number>,ANSW=YES;) and reconfigured.`

  If the configuration of a functional block is not complete **STATUS=CONT** is displayed. The functional block may not be assigned to a board. This is refused by the AMO BCSU with the **Fault message F89**.

Fault message F89

```
F89: THE SPECIFIED FUNCTION BLOCK IS NOT YET FULLY CONFIGURED:

     PLEASE COMPLETE THE CONFIGURATION FIRST WITH THE AMO BFDAT.
```

13.4 Restrictions

- Only one trunking protocol can be configured for each board (AMO CGWB). There are no restrictions on interworking with other functions.
- The entire board must be reconfigured if the changes are made to the configuration.

13.5 Overview of Configuration Steps

An overview of the configuration steps for a HG 3500 V4 common gateway is provided below:

1. Configure functional blocks with the AMO BFDAT (Assistant: **Configuration Management > System Data > Board > CGW Functional Block**)
2. Assign the functional block to a board using the AMO BCSU (Assistant: **Configuration Management > System Data > Board > Board**)
3. Administrate features using the AMO CGWB

14 HiPath Gateway HG 3500 V4 - Changing Parameters with AMO CGWB

IMPORTANT: Any of the settings that can be made here with AMOs are read-only in WBM.

The following branches are supported:

- TYPE ASC - Changing the Payload QoS Setting in HHS
- TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection
- TYPE DMCDATA - Changing the HG 3500 Setting to Support Direct Media Connections
- TYPE DSP - Changing the DSP (Signal Processor) Setting at an HG 3500
- TYPE GLOBIF - Changing the Idle Bit Pattern and Interface-Specific Parameters
- TYPE GWSECTOR - Changing the HG 3500 Sector Number for the Resource Manager
- TYPE MGNTDATA
- TYPE SERVIF - Changing the Login and Password for the Service Access
- TYPE WBMDATA - Changing the Login and Password for WBM
- TYPE JB - Configuring the Jitter Buffer
- Resetting the Parameters to Default Values

14.1 TYPE ASC - Changing the Payload QoS Setting in HHS

In this branch, the Quality of Service for the payload of an access point can be configured. The settings can differ from HG 3500 to HG 3500. If the routers do not support DiffServ, the standard TOS value must be configured without DiffServ. If DiffServ is supported, but not the Siemens CodePoints, the value specified by the network operator must be configured.

In the example, the standard TOS value is set for HG 3500 in LTU 5, mounting slot 91 without DiffServ (see also Table 3-1, “TOS values”).

Configuration Management --> System Data --> IPDA --> IPDA System Data
Enter settings under **Payload Connections** on the **System Data** tab and click **Save**.

```
CHANGE-CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,TOSPL=16;
```

This change is loaded directly to the board and is effective immediately without interrupting operation.

14.2 TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection

See also Chapter 14, “Codec Settings”.

This branches' parameters only apply to **one** HiPath HG 3500 board. Therefore each HG 3500 board could be configured differently in a HiPath 4000 system.

To ensure the usability and the correct diagnosis of the system, these parameters **must** have identical settings (FUNCTION=HG3570) for **all** HG 3500 boards.

In the example, the audio sample size for G.711 and G.729 is set to 60 ms for the common gateway HG 3500 1-5-91. This results in a higher packeting delay, but a comparatively low transmission bandwidth requirement.

Configuration Management --> System Data --> Board --> Board
Click **Search** and select **STMI**.
Set the times for G.711 and G.729 on the **STMI Board Data** tab and click **Save**.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,PRIO=PRIO1,
                   CODEC=G711,RTP=60;
CHNAGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=ASC,PRIO=PRIO2,
                   CODEC=G729,RTP=60;
```

These changes are loaded directly to the HG 3500 and become effective immediately without interrupting operation.

14.3 TYPE DMCDATA - Changing the HG 3500 Setting to Support Direct Media Connections

Use this parameter to set the number of simultaneous direct media connections permitted on a certain HG 3500. The connections are counted both in the HiPath 4000 central system’s software and on the board itself.

Configuration Management --> System Data --> Board --> Board
Click **Search** and select **STMI**.
Make the settings on the **STMI Board Data** tab under **Number of DMC connections** and **Save**.

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**.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=DMCDATA,DMCCONN=30;
```

This change does not become effective on the HG 3500 until this board is restarted with
`RESTART-BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.`

IMPORTANT: Existing links are disconnected.

14.4 TYPE DSP - Changing the DSP (Signal Processor) Setting at an HG 3500

The parameter JITBUFD only takes effect if the parameter JBMODE in the JB branch is set to 0 (LEGACY MODE). JBMODE=0 (=LEGACY MODE) is no longer supported as of HiPath 4000 V4. The jitter buffer size therefore no longer needs to be set.

The parameter VADEN is no longer valid. To configure Voice Activity Detection, you should use the parameter branch TYPE=ASC, parameter VAD (see Section 14.2, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection”).

The parameters in this branch only apply to **one** HiPath HG 3500 module. This means that every HG 3500 module can be configured differently in a HiPath 4000 switch.

However, in order to maintain the ease of use and the diagnostic capability of the system, these parameters **must** be configured **identically** for **all** HG 3500 modules with FUNCTION=HG3570.

In the example, the jitter buffer is set to 100 ms for the common gateway HG 3500 1-5-91.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=DSP,JITBUFD=100;
```

These changes are loaded directly to the HG 3500 and become effective immediately without interrupting operation.

14.5 TYPE GLOBIF - Changing the Idle Bit Pattern and Interface-Specific Parameters

The setting for the physical Ethernet interface may be different for individual HG 3500s.

The Ethernet interface setting must be identical for both connected interface partners (HG 3500 or LAN switches, routers).

IMPORTANT: The setting of a fixed interface partner leads to problems with the "Autonegotiate" setting of the other partner.
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 connected to the HG 3500 does not support autonegotiation or if it does not work reliably, fixed values must be set for the HG 3500’s Ethernet interfaces.

The QoS-relevant parameters are set identically for all HG 3500 modules together with SL100/200 via the AMO SIPCO.

In the example, the Ethernet interface is set to 10 Mbps half duplex and the idle bit pattern is set to 213.

Configuration Management --> System Data --> Board --> Board
Click **Search** and select **Board Name=STMI2** or **Board Name=STMI4**.
Enter appropriate settings on the **STMI Board Data** tab and click **Save**.

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**.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=GLOBIF,PATTERN=213,
                 BITRATE=100MBFD;
```

This change does not become effective on the HG 3500 until this board is restarted with
`RESTART-BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.`

IMPORTANT: Existing links are disconnected.

14.6 TYPE GWSECTOR - Changing the HG 3500 Sector Number for the Resource Manager

In this branch, the parameter GWSECTNO is used to assign the HG 3500 gateway a sector number from the Resource Manager’s sector concept.

Details on the Resource Manager’s sector concept and bandwidth management for gateways can be found in the Resource Manager Service Manual (Complex Solutions, under the “Large Enterprise Gatekeeper” feature).

Configuration Management --> System Data --> Board --> Board
Click **Search** and select **STMI**.
Make the settings on the **STMI Board Data** tab under **Gateway Sector Number** and **Save**.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=GWSECTOR,GWSECTNO=1;
```

This change becomes effective immediately and without interrupting operation.

14.7 TYPE H235DATA - H.235-Security

The H.235 security feature is designed to prevent unauthorized devices setting up connections to a HG 3500 gateway. An example of such a scenario would be a Netmeeting client that wishes to use a HG 3500.

The security concept is based on two mechanisms: When the features are activated, HG 3500 sends a token in each signaling packet (consisting of a password and key, defined in AMO CGWB), to authenticate itself to a receiving HG3550V2 gateway.

In the AMO CGWB a time frame is set. By default, the difference between the time stamp of an arriving H.323 signaling packet and the current time of the receiving HG 3500 cannot exceed 10 seconds.

A time sever is thus required for this feature. If the gateways are in other time zones, this must be set on the HG 3500 boards.

Generation

To activate the H.235 security feature on the board, you set the security flag using the AMO ZANDE. This activates H.235 data in the AMO CGWB on the board.

```
CHANGE-ZANDE:ALLDATA,H235SEC=YES;

CHANGE-CGWB:MTYPE=CGW,LTU=<ltu no>,SLOT=<slot
no>,TYPE=H235DATA,
GLOBID1=<string>,GLOBID2=<string>,TIMEWIN=10,GLOBPW=<
number>;
```

Once you have activated the H.235 security feature with the AMO ZANDE, you must reboot the board to activate the changes.

14.8 TYPE MGNTDATA

The branch **TYPE=MGNTDATA** is used to set up the connection to HiPath 4000 Assistant.This is among other things necessary for the auto restorefunction of the HG 3500.

For trunking connections to HiPath 8000/OpenScape Voice the parameters **MGNTPN** and **BUSPN** are important.

```
CHANGE-CGWB:MTYPE=MGNTDATA,MGNTIP=<ip-address
UW7>,MGNTPN=<port number of UW7>,BUSIP=<ip-address
UW7>,BUSPN=<port number of the backup server>;
```

This command sets up two IP addresses (+ports):

The first IP address **MGNTIP** designates the „Management Station“. This is the IP address under which the HiPath Assistant can be reached. This IP address is important for the single login concept. Logging on to the HG 3500 via the HiPath Assistant is only possible via this IP address.

The second IP address **BUSIP** defines the HBR that is contacted by the HG 3500 at startup during the auto restore.

IMPORTANT: After a reload of the board the values for the ports (**MGNTPN** and **BUSPN**) are not restored. They are set to default. This leads to problems in connection with trunking.

14.9 TYPE SERVIF - Changing the Login and Password for the Service Access

In the parameter tree TYPE=SERVIF you can define the access data for the Command Line Interface.

For more information on CLI please refer to Chapter 16, “Command Line Interface CLI in HG 3500”.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<LTU>,SLOT=<SLOT>,TYPE=SERVIF,LOGINTRM=<Us
er login for terminal mode>,PASSW=<Password for terminal
mode>;
```

The standard login data is:

Login: TRM (parameter (**LOGINTRM**)

Password: PUBLIC (parameter **PASSW**)

14.10 TYPE WBMDATA - Changing the Login and Password for WBM

WBM access can be configured in this branch.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<LTU>,SLOT=<SLOT>,TYPE=WBMDATA,LOGINWBM=<U
ser login for WBM connection>,PASSWWBM=<Password for WBM
connection>,ROLE=<Role of the WBM user; sets access rights>;
```

Role	Rights
ADMIN	Administrator (default value)
ENGR	Developer (access to all features)
READONLY	Administrator with read-only access
SU	Superuser (access to all features)

Table 19 WBM rights

The data for initial login as ENGR is:

User name: `HP4K-DEVEL`

Password: `Siemens2000`

14.11 TYPE JB - Configuring the Jitter Buffer

As of HiPath 4000 V4, only the adaptive jitter buffer (JBMODE=2) and the static jitter buffer (JBMODE=1) are supported in the HG 3575 V4 gateway. If JBMODE=0 (LEGACY MODE) is set in the AMO STMIB, this is mapped to the static jitter buffer (JBMODE=1) in the gateway.

A basic understanding of procedures and configuration parameters is required to perform configuration. Refer to Section 2.5, “Jitter Buffer”.

The adaptive jitter buffer that reduces delays is set by default.

Configuration Management --> System Data --> IPDA --> IPDA Access Point
Click **Search** and select the access point.
Enter the parameter on the **General** tab under **Jitter Buffer** and **Save**.

```
CHANGE-CGWB:MTYPE=CGWB,LTU=5,SLOT=91,TYPE=JB,

AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4,
              AVGDLYD=60,MAXDLYD=200, JBMODE=2;
```

WBM **Explorers > Payload > HW Modules > Edit DSP Jitter Settings**

These changes are started directly on the access point and become effective when the next connection is set up.

14.12 Resetting the Parameters to Default Values

If the parameters of one or all branches of the STMI2/4 data are to be reset to default values, e.g. after being changed temporarily for diagnostic work, this can be performed in the INITCGW branch. The example sets all DMCDATA parameters to their default values.

Initialization and reloading (where required) can only be performed in expert mode.
Expert Mode --> HiPath 4000 --> HiPath 4000 Expert Access --> Open ...<IP> using AMO
(see AMO command)

```
CHANGE-CGWB:MTYP=INITCGW,LTU=5,EBT=91,TYP=DMCDATA;
```

The changes under TYPE ASC, DSP, MGNTDATA, SIPTRERH, WBMDATA, **DLSDATA** and JB **become effective immediately** without interrupting operation.

Changes under TYPE DMCDATA, GKDATA, GLOBIF, GWDATA, GWSECTOR, H235DATA, SIPTRSSA and **DLSDATA become effective after the HG 3500 has been restarted** with
`RESTART-BSSU:ADDRTYPE=PEN,LTU=5,SLOT=91.`

Note: Existing links are disconnected.

DLSDATA

DLSIPADR & DLSPORT : become effective after CGW restart

DLSACPAS : become effective immediately without interrupting operation

15 Codec Settings

15.1 HFA and Trunking

A priority list of the codecs is configured in the AMO CGWB for HG 3500, and accordingly in the AMO STMIB for HG 3575. During codec negotiations, the gateways use the codecs configured in this way.

Examples:

- Gateway is a DMC endpoint
- Master connections for HFA and IP trunking

Example

- HG 3500 (STMI)

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,UDPPRTLO=29100,UDPPRTHI
=29339,TOSPL=0,TOSSIGNL=0,
TCPPRTLO=0,TCPPRTHI=0,T38FAX=YES,RFCFMOIP=YES,RFCDTMF=YES,RED
RFCTN=YES,PRIO=PRIO1,CODEC=G711,VAD=YES,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO2,CODEC=G711U,
VAD=YES,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO3,CODEC=G729A,
VAD=NO,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO4,CODEC=G729B,
VAD=YES,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO5,CODEC=G729AB
,VAD=YES,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO6,CODEC=NONE,V
AD=NO,RTP="20";
```

```
CHANGE-
CGWB:MTYPE=CGW,LTU=3,SLOT=11,TYPE=ASC,PRIO=PRIO7,CODEC=NONE,V
AD=NO,RTP="20";
```

- HG 3575 (NCUI)

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,TOSPL=48,PRIO1,CODEC=G771,V
AD=YES,RTP="20";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO2,CODEC=G771U,VAD=
YES,RTP="20";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO3,CODEC=G729AB,VAD
=YES,RTP="40";
```

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO4,CODEC=G729B,VAD=
YES,RTP="20";
```

```
CHA-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO5,CODEC=NONE;
```

```
CHA-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO6,CODEC=NONE;
```

```
CHA-STMIB:MTYPE=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO7,CODEC=NONE;
```

15.2 IPDA

For IPDA, the codecs for the master connection are switched by DNIL and configured in AMO SDAT / AMO TDCSU, etc., i.e. in the user/trunk data of the affected devices (see IP Distributed Architecture (IPDA) and Access Point Emergency (APE), Section 4.9, “Configuring Subscriber, CO/Tie Trunk Circuits in Access Points”).

IMPORTANT: This means that the codecs do not need to be configured in the AMOs CGWB and STMIB for the IPDA master connection.

For IPDA connections, the codecs are configured as previously described in the AMOs STMIB or CGWB (see also Section 12.5, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, Voice Activity Detection and T.38 Fax” and Section 14.2, “TYPE ASC - Setting the Codec List for DMC Connections, RTP Packet Size, and Voice Activity Detection”).

16 Multiple Feature Support Configuration at the Common Gateway (Example)

16.1 Important Information

- If the function IPDA (HG3570) is configured on an STMI board, the IP address of the common gateway must be assigned with the AMO BCSU. For all other functions of the board, the IP address must be assigned with the AMO CGWB.
- If several functions are defined in a function block (IPDA and others), the IP address for IPDA must be set with AMO BCSU, for the other functions the **same** IP address must be configured using the AMO CGWB!
- **VLAN settings** in AMO CGWB: When MFS is configured, the following AMOs are used:
  - MFS with IPDA functionality: AMO SIPCO
  - MFS without IPDA functionality: AMO CGWB
- **Trunking protocols**
  Only one trunking protocol can be configured for each common gateway board (either SIP or H323)! If both protocols should be used for trunking, individual boards must be used.

16.1 Configuring Functional Blocks with the AMO BFDAT

- Functional block 1: IPDA (HG3570)
- Functional block 2: IPDA (HG3570), IP trunking (HG3550) and HFA subscriber (HG3530)
- Functional block 3: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 4: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 5: IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)
- Functional block 6: IP trunking (HG3550) and HFA subscriber (HG3530)
- Functional block 7: IP trunking, HFA subscriber (HG3530) and reserve HFA subscriber (HG3530R)

Functional block 1

/* Functional block 1: Adding the IPDA function (HG3570)

```
ADD-BFDAT:FCTBLK=1,FUNCTION=HG3570,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 120 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3570,BCHLCNT=120;
```

>>>>> End configuration of this block

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

Functional block 2

/* Functional block 2: Adding the functions IPDA (HG3570), IP trunking (HG3550) and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=2,FUNCTION=HG3570&HG3550&HG3530,BRDBCHL=BCHAN;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with three units (=30 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> HFA with 60 circuits with 60 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=2,FUNCTION=HG3530,LINECNT=60,BCHLCNT=60;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=2,ANSW=YES;
```

Functional block 3

/* Functional block 3: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=3,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with three units (=30 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> WAML

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=WAML,UNITS=3;
```

>>>>> HFA with 30 circuits with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3530,LINECNT=30,BCHLCNT=30;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=3,ANSW=YES;
```

Functional block 4

/* Functional block 4: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3550,LINECNT=1,UNITS=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA with 70 circuits with 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3530,LINECNT=70,BCHLCNT=70;
```

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=YES;
```

Functional block 5

/* Functional block 5: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=5,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit with 10 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3550,LINECNT=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=WAML;
```

>>>>> HFA with 140 circuits with 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=5,FUNCTION=HG3530,LINECNT=140,BCHLCNT=70;
```

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=5,ANSW=YES;
```

Functional block 6

/* Functional block 6: Adding the functions IP trunking (HG3550) and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=6,FUNCTION=HG3550&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IP trunking with one circuit with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3550,LINECNT=1,UNITS=3;
```

>>>>> HFA with 90 circuits with 90 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3530,LINECNT=90,BCHLCNT=90;
```

>>>>> End configuration of this block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=6,ANSW=YES;
```

Functional block 7

/* Functional block 7: IP trunking, HFA subscriber function (HG3530) and reserve HFA subscriber (HG3530R)

IMPORTANT: The reserved HFA B channels must be specified during configuration of the HG3530 function as subscriber B channels are not accepted during reservation.

```
ADD-BFDAT:FCTBLK=7,FUNCTION=HG3550&HG3530&HG3530R,BRDBCHL=BCHAN120;
```

>>>>> HFA with 80 circuits with 80 B channels and 20 reserve B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3530,LINECNT=80,BCHLCNT=100;
```

>>>>> Reserve HFA subscriber with 20 circuits

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3530R,LINECNT=20;
```

>>>>> IP trunking with 10 circuits with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=7,FUNCTION=HG3550,LINECNT=10,UNITS=1;
```

Displaying all functional blocks

```
DISPLAY-BFDAT;

H500:  AMO BFDAT STARTED
```

```
--------------------------------------------------------------------------------
| FCTBLK =  1    BRDBCHL: BCHAN120                    STATUS=      OK           |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS ??  BCHLCNT 120  TOTAL BCHAN 120   |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  2    BRDBCHL : BCHL120                    STATUS=      OK           |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN 30    |
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN 30    |
|  3rd FUNCT : HG3530      60 LINES    UNITS 60  BCHLCNT  60  TOTAL BCHAN 60    |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  3    BRDBCHL : BCHL120                    STATUS=      OK           |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN 30    |
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN 30    |
|  3rd FUNCT : WAML         1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN 30    |
|  4th FUNCT : HG3530      30 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN 30    |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120                    STATUS=      OK           |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN 30    |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN 10    |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN 10    |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN 70    |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  5    BRDBCHL : BCHL120                    STATUS=    CONT           |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN 30    |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN 10    |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10   |
|  4th FUNCT : HG3530     140 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70   |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  6    BRDBCHL : BCHL120                     STATUS=      OK          |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT  30  TOTAL BCHAN  30   |
|  2nd FUNCT : HG3530      90 LINES    UNITS 90  BCHLCNT  90  TOTAL BCHAN  90   |
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
| FCTBLK =  7    BRDBCHL : BCHL120                     STATUS=      OK          |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3530      80 LINES    UNITS 80  BCHLCNT 100  TOTAL BCHAN 100   |
|  2nd FUNCT : HG3530R     20 LINES    UNITS 20  BCHLCNT   0  TOTAL BCHAN   0   |
|  3rd FUNCT : HG3550      10 LINES    UNITS 10  BCHLCNT  10  TOTAL BCHAN  10   |
--------------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
DISPLAY COMPLETED;
  <
```

16.2 Configuring the Common Gateway Board with the AMO BCSU

Assignment for functional block 1

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=2,SLOT=37,PARTNO=Q2316-X10,FCTID=1,FCTBLK=1,IPADDR=198.16.16.45;
```

```
DISPLAY-BCSU:TYPE=TBL,LTG=1,LTU=2;
```

```
H500:  AMO BCSU  STARTED
ADDRESS :  LTG  1   LTU 2    SOURCE GROUP 1    ALARMNO-LTU 0
-----+-----------+--------+---+-+-+----+-+------------+------------+-----------
     |           |        |   |S|H|AL-| |            |            |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |    HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE INFO  | STATUS
-----+-----------+--------+---+-+-+----+-+------------+------------+-----------
```

```
  19 | Q2258-X    ACGEN            0|*| AVAILABLE |           | NPR
  25 | Q2205-X    WAML      1  A   0|*|           |           | NPR
  31 | AVAILABLE                   0| | AVAILABLE |           |
  37 | Q2316-X10  STMI2     1  A   0|*|           |           | NPR
     +------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 198. 16. 16. 45      B-CHANNELS : 120    BCHLCNT :   2
     | BLOCK NO   :   1                  PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA   1 LINES   B-CHANNELS : 120    BCHLCNT :   2
     +------------------------------+-+-----------+-----------+-----------
  43 | Q6401-X    PBCDG-FU  3  A   0|*|           |           | NPR
  49 | AVAILABLE                   0| | AVAILABLE |           |
  55 | Q2214-X    TMOM2        A   0|*|           |           | NPR
  61 | Q2195-X    DIU-N4    1  A   0|*|           |           | NPR
  67 |                             0| |           |           |
  73 | Q2248-X    LTUCE            0|*| AVAILABLE |           | NPR
  79 | Q2096-X200 DIU-S2       A   0|*|           |           | NPR
  85 | Q2096-X200 DIU-S2       A   0|*|           |           | NPR
  91 | Q2096-X200 DIU-S2       A   0|*|           |           | NPR
  97 | Q2096-X200 DIU-S2       A   0|*|           |           | NPR
 103 | AVAILABLE                   0| | AVAILABLE |           |
 109 | AVAILABLE                   0| | AVAILABLE |           |
 115 | Q2096-X200 DIU-S2       A   0|*|           |           | NPR
 121 | Q2174-X    STMD         A   0|*|           |           | NPR
DISPLAY COMPLETED;
```

Assignment for functional block 2

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=31,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=2,IPADDR=198.16.16.31;
```

Assignment for functional block 3

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=37,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=3,IPADDR=198.16.16.37;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=4,IPADDR=198.16.16.43;
```

Assignment for functional block 5

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=49,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=5,IPADDR=198.16.16.49;
```

Assignment for functional block 6

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=55,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=6,IPADDR=198.16.16.55;
```

Assignment for functional block 7

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=61,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=7,IPADDR=198.16.16.59;
```

Converting reserved HFA circuits to usable circuits

```
CHANGE-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=61,CHNGRSLN=13;

DISPLAY-BCSU:TYPE=TBl,LTG=1,LTU=1;

H500:  AMO BCSU  STARTED


ADDRESS :  LTG  1   LTU 1    SOURCE GROUP 1    ALARMNO-LTU 0

-----+----------+-------+---+-+-+---+-+-----------+-----------+-----------

     |          |       |   |S|H|AL-| |           |           |
     | ASSIGNED | MODULE |FCT|E|W|ARM| | INSERTED   |    HW-     | MODULE
 PEN | MODULE   | TYPE  |ID |C|Y|NO | | MODULE     |STATE INFO | STATUS
-----+----------+-------+---+-+-+---+-+-----------+-----------+-----------

  19 | Q7065-X    APPS              0|*| AVAILABLE |           | NPR
  25 | Q2117-X    SLMS          A   0|*|           |           | NPR
  31 | Q2316-X10  STMI2      1  A   0|*|           |           | NPR
     +-----------------------------+-+-----------+-----------+-----------
     | IP ADDRESS : 198. 16. 16. 31        B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO    :   2                   PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES  B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES  B-CHANNELS :  30    BCHLCNT :  30
```

```
   |  3rd FUNCT  : STMI-HFA2    60 LINES   B-CHANNELS :  60    BCHLCNT :  60
   +--------------------------------+-+------------+------------+-----------
37 | Q2316-X10  STMI2      1   A   0|*|            |            | NPR
   +--------------------------------+-+------------+------------+-----------
   | IP ADDRESS : 198. 16. 16. 37         B-CHANNELS : 120    BCHLCNT : 120
   | BLOCK NO   :   3                     PRERESERVED LINES ASSIGNED     NO
   |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
   |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
   |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
   |  4th FUNCT  : STMI-HFA2    30 LINES   B-CHANNELS :  30    BCHLCNT :  30
   +--------------------------------+-+------------+------------+-----------
43 | Q2316-X10  STMI2      1   A   0|*|            |            | NPR
   +--------------------------------+-+------------+------------+-----------
   | IP ADDRESS :  198. 16. 16. 43         B-CHANNELS : 120    BCHLCNT : 120
   | BLOCK NO   :   4                     PRERESERVED LINES ASSIGNED  :  NO
   |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
   |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
   |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
   |  4th FUNCT  : STMI-HFA2    70 LINES   B-CHANNELS :  70    BCHLCNT :  70
   +--------------------------------+-+------------+------------+-----------
49 | Q2316-X10  STMI2      1   A   0|*|            |            | NPR
   +--------------------------------+-+------------+------------+-----------
   | IP ADDRESS : 198. 16. 16. 49         B-CHANNELS : 120    BCHLCNT : 120
   | BLOCK NO   :   5                     PRERESERVED LINES ASSIGNED  :  NO
   |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
   |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
   |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
   |  4th FUNCT  : STMI-HFA2   140 LINES   B-CHANNELS :  70    BCHLCNT :  70
   +--------------------------------+-+------------+------------+-----------
55 | Q2316-X10  STMI2      1   A   0|*|            |            | NPR
   +--------------------------------+-+------------+------------+-----------
   | IP ADDRESS :  198. 16. 16. 55        B-CHANNELS : 120    BCHLCNT : 120
   | BLOCK NO   :   6                     PRERESERVED LINES ASSIGNED  :  NO
```

```
     |  1st FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI-HFA2    90 LINES   B-CHANNELS :  90    BCHLCNT :  90
     +--------------------------------+-+-------------+------------+------------
  61 | Q2316-X10  STMI2      1   A   0|*|             |            | NPR
     +--------------------------------+-+-------------+------------+------------
     | IP ADDRESS :  198. 16. 16. 59       B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   7                    PRERESERVED LINES ASSIGNED  : YES
     |  1st FUNCT  : STMI-HFA2    93 LINES   B-CHANNELS : 100    BCHLCNT : 100
     |  2nd FUNCT  : STMI-HFA2R    7 LINES   B-CHANNELS :   0    BCHLCNT :   0
     |  3rd FUNCT  : STMI2-IPGW   10 LINES   B-CHANNELS :  10    BCHLCNT :  10
     +--------------------------------+-+-------------+------------+------------
  67 | AVAILABLE                     0| | AVAILABLE   |            |
  73 | Q2248-X    LTUCE              0|*| AVAILABLE   |            | NPR
  79 | Q2164-X    SLMO16     1   A   0|*|             |            | NPR
  85 | Q2168-X    SLMO24     1   A   0|*|             |            | NPR
  91 | Q2153-X100 SLMQ           A   0|*|             |            | NPR
  97 | Q2150-X    SLMB           A   0|*|             |            | NPR
 103 | Q2480-X    SLMAR          A   0|*|             |            | NPR
 109 | Q2246-X    SLMA24         A   0|*|             |            | NPR
 115 | Q2025-X300 TMBD           A   0|*|             |            | NPR
 121 | AVAILABLE                     0| | AVAILABLE   |            |
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
DISPLAY COMPLETED;
```

Seven common gateway boards (in this case: Q2316-X10, STMI2) have been configured.

16.3 Configuring SIP Trunking

Configuring SIP trunking on the STMI2 board in 1-1-55:

```
ADD-CGWB:LTU=1,SLOT=55,SMODE=NORMAL,IPADDR=198.16.16.55,NET-
MASK=255.255.255.0,TRPRSIP=30;
```

IMPORTANT: Only one trunking protocol can be configured for each common gateway board.

16.4 Completed and Uncompleted Functional Block

16.4.1 Uncompleted functional block

/* Functional block 4: Adding the functions IPDA (HG3570), IP trunking (HG3550), WAML and HFA subscriber (HG3530)

```
ADD-BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BRDBCHL=BCHAN120;
```

>>>>> IPDA with 30 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3570,BCHLCNT=30;
```

>>>>> IP trunking with one circuit and one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3550,LINECNT=1,UNITS=1;
```

>>>>> WAML with one unit (=10 B channels)

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA with 70 circuits and 70 B channels

```
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=4,FUNCTION=HG3530,LINECNT=70,BCHLCNT=70;
```

>>>>> Do not end configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=NO;
```

Displaying a functional block

```
DISPLAY-BFDAT:FCTBLK=4;

H500:  AMO BFDAT STARTED
--------------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120                      STATUS=   CONT          |
--------------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30   |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10   |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10   |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70   |
--------------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS
DISPLAY COMPLETED;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=4,IPADDR=198.16.16.43;

H500:  AMO BCSU  STARTED

F89: THE GIVEN FUNCTIONAL BLOCK IS NOT COMPLETELY CONFIGURED.

     PLEASE FINISH CONFIGURATION BY MEANS OF AMO_BFDAT FIRST.

AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT

ADD NOT COMPLETED;
```

IMPORTANT: If the configuration of a functional block with the AMO BFDAT is not completed, the block cannot be assigned to any board with the AMO BCSU.
The functional block must be completely configured with the AMO BFDAT before the command can be successfully run.

16.4.2 Completed configuration block

>>>>> End configuration of block

```
CHANGE-BFDAT:CONFIG=OK,FCTBLK=4,ANSW=YES;
```

Displaying a functional block

```
DISPLAY-BFDAT:4;

H500:  AMO BFDAT STARTED

------------------------------------------------------------------------

| FCTBLK =  4    BRDBCHL : BCHL120                     STATUS=      OK         |

------------------------------------------------------------------------

|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT  30  TOTAL BCHAN  30   |

|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10   |

|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT  10  TOTAL BCHAN  10   |

|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT  70  TOTAL BCHAN  70   |

------------------------------------------------------------------------

AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR CGW BOARDS

DISPLAY COMPLETED;
```

Assignment for functional block 4

```
ADD-BCSU:TYPE=IPGW,LTG=1,LTU=1,SLOT=43,PARTNO=Q2316-X10,FCTID=1,FCT-
BLK=4,IPADDR=198.16.16.43;

H500:  AMO BCSU  STARTED

H01: BD  1.1 . 43 ASSIGNED

AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT

ADD COMPLETED;
```

17 Command Line Interface CLI in HG 3500

17.1 General Information

The common gateway supports a **C**ommand **L**ine **I**nterface (CLI) for installation and basic configuration, e.g. IP infra structure. In V.24 CLI it is possible to change security relevant data (e.g. SSL Configuration), because the V.24 is considered to be secure. Additionally the CLI allows the monitoring of important counters and statistics.

The CLI can be accessed via V.24. The CLI can not be accessed via Telnet because it is an unsecure protocol.

To get an overview of the commands type in the command `help` and you get an alphabetic list of all commands.

Please refer to Section 14.9, "TYPE SERVIF - Changing the Login and Password for the Service Access" on how to configure the access data for CLI.

The basic function of the CLI are described below. In the following sections the CLI commands are divided into seven categories:

- General Operations
- Access control
- Gateway Setup
- Image/File Handling
- Maintenance
- SSL for WBM
- DLS

17.2 General Operations

When starting a session the administrator is asked for authentication. That is done by entering the admin name and the password.

- To leave the session use the

  ```
  logout
  ```

  command.
- The list of all supported commands except the hidden commands can be obtained with:

  ```
  help
  ```

17.3 Access control

- The configuration write access has to be acquired before a store, upload or download command can be done. Because of the implemented “soft lock“ handling, at first a check if somebody else has set the write access is required.

```
who has write access
get write access
release write access
```

17.4 Gateway Setup

To permit system initialisation and basic management configuration activities following commands are needed.

- Setting and changing the gateway name:

  ```
  set hostname <hostname>
  ```

- Setting and changing the IP-Address for the ethernet port:

  ```
  set ip address <ip address>
  set ip subnet <ip subnet mask>
  ```

  A set or a change of the IP-address or IP subnet for the ethernet port will probably require a gateway reboot to become effective.

- Setting and changing the IP-address of the default gateway from static routes table:

  ```
  set default gateway <ip address>
  ```

- Display/change choosen identifier:

  ```
  get id <parameter name>
  set id <parameter name>
  ```

hostname

The parameter `hostname` > terms an arbitrary name for the gateway and it must be a string of characters (e.g. set hostname Gateway1). It corresponds with the boot line parameter "targetname".

ip address

The parameter <`ip address`> is a string in the form of x.x.x.x and x is an integer (e.g. 1.2.3.4)

ip subnet mask

The parameter <`ip subnet mask`> is a string in the form of x.x.x.x and x is an integer between 0 and 255 (e.g. 255.255.255.224).

17.5 Image/File Handling

In common gateway software configuration and distribution as well as upload and download of configuration data via CLI is not required because it is done via WBM.

Additionally operations for analysing event and trace data are supported.

The trace /event logs are available as:

```
/trace/trace.txt
/trace/trace.bak

/evtlog/evtlog.txt
/evtlog/evtlog.bak
```

17.6 Maintenance

The maintenance commands permit the current operational status of the gateway to be inspected, and provides access to diagnostic tools and interface and gateway controls.

Display

- Commands which provide information on the gateway’s software configuration:

  ```
  show version
  show uptime
  ```

- Display of IP-address, subnet and gateway:

  ```
  show all parameters
  ```

- Display of hostnames and IP-addresses:

  ```
  show host
  ```

- Get the name of the gateway:

  ```
  show hostname
  ```

- Display of arp-cache:

  ```
  show arp cache
  ```

  It is also stored in the bootline as targetname.

- Display of the IP address and subnetmask for the ethernet port:

  ```
  show ip address
  show ip subnet
  ```

- Showing the time will display the time and the date:

  ```
  show time
  ```

- Command to get the IP address of the default gateway from the static routes table:

  ```
  show default gateway
  ```

- Command to display the static routes entries:

  ```
  show routes
  ```

- To display the statistics of the interface table:

  ```
  show if counters
  ```

- To list all existing interfaces:

  ```
  show interfaces
  ```

- To get admin and operating states:

  ```
  show if states
  ```

Ping and tracert

- Diagnosis Commands:

  ```
  ping <ip address>
  ```

Target shell

- vxWorks shell logon/logout:

  ```
  shell
  exit
  ```

Gateway Reboot

From the administrator point of view two different ways of a reboot command are of interest. At first there is the need to reboot the gateway with the current configuration. On the other side there could be the need to support a configuration data exchange, i.e. to take a configuration data file from extern or to skip the latest configuration data storage and take the next older one.

It is in the responsibility of the administrator to coordinate a gateway reboot!

- Normal reboot of the gateway, using the current configuration data:

  ```
  reset
  ```

- Reset any configuration data to factory defaults and reboot:

  ```
  reset factory
  ```

- Special reboot of the gateway using an existing self-extracting image in order to complete a software download:

  ```
  activate software
  ```

17.7 SSL for WBM

SSL for WBM (i.e. https) is enabled in the factory delivered status. It cannot be disabled.

To permit a basic configuration of SSL following commands are needed.

- Display the fingerprint of the currently active certificate for WBM access via https.

  ```
  show fingerprint
  ```

  Before accepting a certificate warning in the browser, it is strongly recommended that the administrator should compare the fingerprint of the certificate displayed in the browser against the fingerprint shown in CLI. The certificate must be accepted only, if both fingerprints are identical!

17.8 DLS

- Set the IP address of the DLS server

  ```
  set dls ip_address <ip address[:port]>
  ```

  You can set the IP address of the DLS server manually with `set dls ip_address` (optional). The IP address is automatically set if you use the function **IP Devices > IP Device Interaction > Scan IP Devices** (activate the checkbox **Send DLS Address** in the **"Configuration"** tab for this).

- Show the IP address of the DLS server

  ```
  show dls ip_address
  ```

  The gateway contains a DLS client. This setting makes sure that the gateway automatically recognizes the IP address of the DLS client.

- DLS PIN

  IP Devices > IP Device Management > IP Device Configuration > "DLS Connectivity"

Three security settings are available under **PIN Mode** for creating a virtual device in the DLS:

– **No PIN**,

– **Default PIN**,

– **Individual PIN**.

See also Chapter 11, “DLS Client Bootstrapping”.

If you set **dls pin_required** to **TRUE** in the gateway, the gateway declines a connection if **No PIN** is set in the DLS. This setting offers added security.

The PIN is automatically generated by the DLS and displayed in the **Default PIN:** field in the DLS under **Administration > Workpoint Interface Configuration > "Secure mode"** tab. It has the same function as a password.

```
set dls pin_required <value>
```

Possible values: **0**, **1**

```
show dls pin_required
```

Possible values: **FALSE**, **TRUE**

- Activate the DLS PIN

  ```
  activate dls pin <pin>
  ```

  If you select **Default PIN** or **Individual PIN** as the PIN mode in the DLS, you must use this command to enter the PIN displayed in the DLS.

- Bootstrapping

  The command `reset dls bootstrapping` resets the gateway defaults for DLS client bootstrapping; you can then repeat bootstrapping (see also Chapter 11, “DLS Client Bootstrapping”).

  ```
  reset dls bootstrapping
  ```

- DLS client status

  Shows the value "secure" or "insecure". This is followed by a number in brackets which is used for diagnostic purposes.

  ```
  show dls_client_state
  ```

  Possible values: **secure**, **insecure**

- Contact the DLS server

  ```
  contact dls
  ```

  This command tries to contact the DLS server.

  You only need to do this to start DLS client bootstrapping after manually configuring the DLS server’s IP address with `set dls ip_address`.

Otherwise, you can use `contact dls` to test if communication is possible between the gateway and DLS server. An appropriate message appears.

0

A PIN is not needed. **"No PIN"** is set as the PIN mode in the DLS.

1

A PIN is needed. **"Default PIN"** or **"Individual PIN"** is set as the PIN mode in the DLS.

FALSE

A PIN is not needed. **"No PIN"** is set as the PIN mode in the DLS.

TRUE

A PIN is needed. **"Default PIN"** or **"Individual PIN"** is set as the PIN mode in the DLS.

secure

DLS client bootstrapping has already taken place.

insecure

DLS client bootstrapping has not yet been performed or was unsuccessful.

17.9 Changing the Login and Password for WBM/CLI

From HiPath 4000 V4 onwards for CLI login, the same accounts as for WBM login have to be used. The accounts can be set up and changed via AMO CGWB. The parameter ROLE defines the access rights.

IMPORTANT: As of HiPath 4000 V4, CLI is not released in two stages anymore!

```
CHANGE-
STMIB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=WBMDATA,LOGINWBM=<use
r login for wbm connection>,PASSWWBM=<password for wbm
connection>,ROLE=<role of the wbm user>;
```

The initial login as ENGR is

```
username: HP4K-DEVEL
Passowrd: Siemens2000
```

After successful login the following message appears:

```
Welcome to the HG 3575 V4.0 <LW-version> Command Line
Interpreter.
```

```
   vxTarget>
```

<LW-version>

<LW-version> holds the currently loaded loadware version number (e.g. L0-TOS.10.030-004)

18 Command Line Interface CLI at HG 3575 V4

Please refer to IP Distributed Architecture (IPDA) and Access Point Emergency (APE), Chapter 1, “Local Access Point Administration at CLI via Terminal”.

19 SNMP Support HG 3500 / HG 3575

The HiPath HG 3500 module supports the request of data via SNMP. Figure 19 shows the MIB tree.

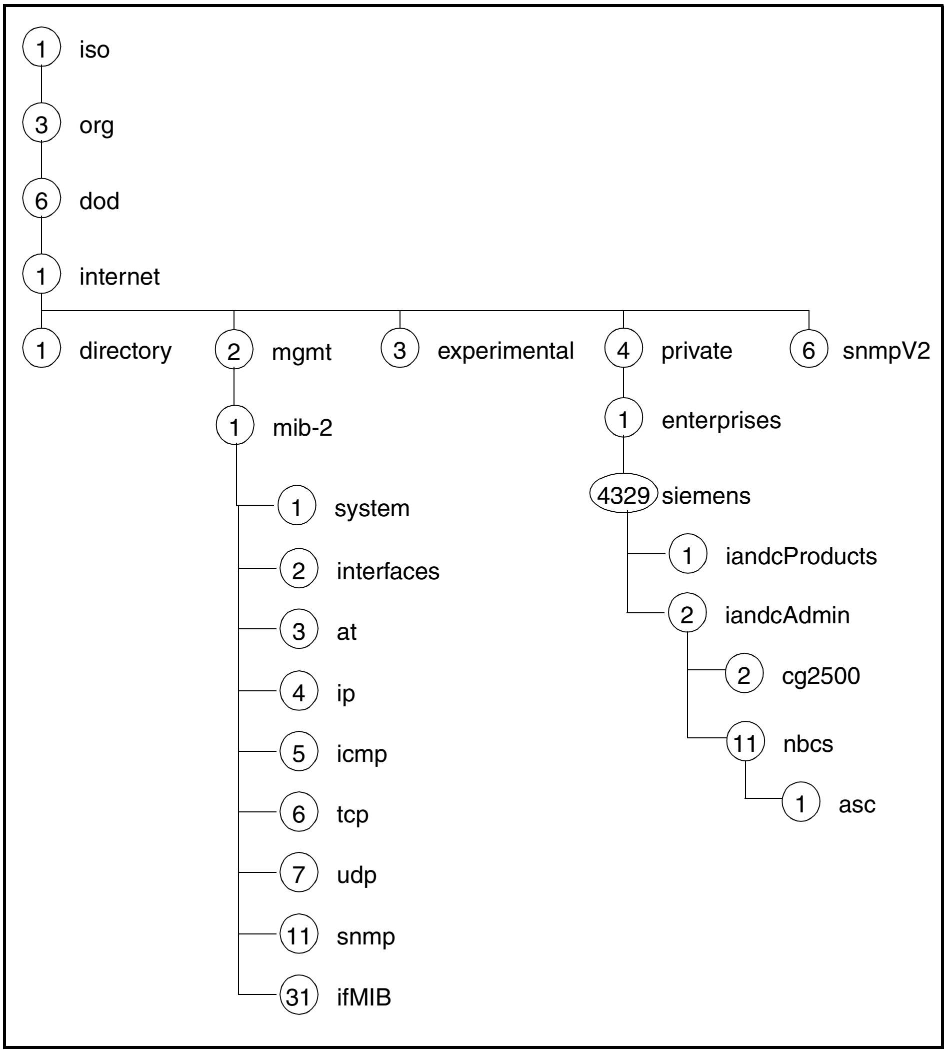


Figure 19 MIB tree

The standards MIB (MIB-2) and the Private MIB for Audio Stream Control (ASC) are supported

MIB-2:

- (1) System Group (RFC1213)
- (2) Interfaces Group (RFC2233) [EthernetifType: 6]
- (3) AT Group (RFC1213)
- (4) IP Group (RFC2011/RFC1213)

- (5) ICMP Group (RFC2011)
- (6) TCP Group (RFC2012)
- (7) UDP Group (RFC2013)
- (11) SNMP Group (RFC1213)
- (31) ifMIB Group (RFC2233)

MIB-ASC:

Implemented MIB objects:

- **ASC Statistics Group** (ascStats)

```
Implemented objects: { asc 1 }

  ascStatsOverall                    OBJECT-TYPE ::= { ascStats 1 }
  ascAllOutgoingRTPpackets           OBJECT-TYPE ::= { ascStatsOverall 1 }
    Outgoing RTP packets (overall)
  ascAllOutgoingRTPpacketsLost       OBJECT-TYPE ::= { ascStatsOverall 2 }
    Outgoing RTP packets lost (overall).
  ascAllBytesSent                    OBJECT-TYPE ::= { ascStatsOverall 3 }
    Total bytes sent.
  ascAllIncomingRTPpackets           OBJECT-TYPE ::= { ascStatsOverall 4 }
    Incoming RTP packets (overall).
  ascAllIncomingRTPpacketsLost       OBJECT-TYPE ::= { ascStatsOverall 5 }
    Incoming RTP packets lost (overall).
  ascAllBytesReceived                OBJECT-TYPE ::= { ascStatsOverall 6 }
    Total bytes received

  ascStatsPerCall                    OBJECT-TYPE ::= { ascStats 2 }
  ascMaxCalls                        OBJECT-TYPE ::= { ascStatsPerCall 1}
    Max. number of calls (channels) processed by ASC.

  ascStatsPerCallTable               OBJECT-TYPE ::= { ascStatsPerCall 2}
    The table of per-call ASC statistics.
  ascStatsPerCallEntry               OBJECT-TYPE ::= { ascStatsPerCallTable 1 }
    The ASC statistics about one resource
  SEQUENCE
  {
    ascCallIndex                     INTEGER,
   A unique value for each interface.  Its value ranges between 1 and the value of ascMaxCalls
  ascPeerCanonicalName              OCTET STRING,
   NPCI value for the call
  ascDestIP                         OCTET STRING,
   The destination IP address (of corresponding HG 3500/3575)
  ascBeginTime                      OCTET STRING,
   When the last call started
  ascEncoder                        INTEGER,
   Encoder used with this call
  ascDecoder                        INTEGER,
   Decoder used with this call
  ascOutgoingRTPpackets             Counter32,
   Outgoing RTP packets (per-call)
  ascOutgoingRTPpacketsLost         Counter32,
   Outgoing RTP packets lost (per-call)
  ascBytesSent                      Counter32,
   Total bytes sent
  ascIncomingRTPpackets             Counter32,
   Incoming RTP packets (per-call)
  ascIncomingRTPpacketsLost         Counter32,
   Incoming RTP packets lost (per-call)
  ascBytesReceived                  Counter32,
   Total bytes received
  ascAverageNetworkDelay            Gauge32,
   Average network delay for this call (over duration) measured in 1/65536 sec
  ascJitter                         Gauge32,
   Cumulated Jitter of this call measured in timestamp units (0.125 ms)
  ascMaxFractionOutgoing            Counter32,
   Maximal fraction of outgoing lost packets to sent packets of this call
  ascCumLatePacketCount             Counter32,
}  Cumulated late packets (counted as lost packets)
  ascRndTripNetworkDelay            Gauge32
   Actual round trip delay in ms (observation period 5s)
  ascFractionOutgoing               Gauge32
   Actual fraction outgoing in % (observation period 5s)
  ascActualJitter                   Gauge32
   Actual Jitter in ms (observation period 5s)
```

```
    }
```

- **ASC Config Group** (ascConfig) not relevant for IPDA components

```
Implemented objects: { asc 2 }
```

```
ascUdpPortLow                        OBJECT-TYPE ::= { ascConfig 1 }
```

Low boundary of RTP/RTCP ports

```
ascUdpPortHigh                       OBJECT-TYPE ::= { ascConfig 2 }
```

High boundary of RTP/RTCP ports

```
ascTcpPortLow                        OBJECT-TYPE ::= { ascConfig 3 }
```

Low boundary of TCP ports (fax)

```
ascTcpPortHigh                       OBJECT-TYPE ::= { ascConfig 4 }
```

High boundary of TCP ports (fax)

```
ascDtmfDefaultToneLength             OBJECT-TYPE ::= { ascConfig 6 }
```

Default length of the DTMF tones

```
ascG711MaxRecvBytes                  OBJECT-TYPE ::= { ascConfig 7 }
```

Maximum number of bytes of G.711 coded RTP data (w/o header)

```
ascG723MaxRecvBytes                  OBJECT-TYPE ::= { ascConfig 8 }
```

Maximum number of bytes of G.723 coded RTP data (w/o header)

```
ascG729MaxRecvBytes                  OBJECT-TYPE ::= { ascConfig 9 }
```

Maximum number of bytes of G.729 coded RTP data (w/o header)

```
ascPacketSizeTotalFractionLostWeight OBJECT-TYPE ::= { ascConfig 10 }
```

Factor for smoothing the varying fraction lost of RTP packets in 10th of percents, i.e. 1000 is 100.0%. Default: 300 (30%)

```
ascPacketSizeMinFractionLost         OBJECT-TYPE ::= { ascConfig 11 }
```

Lower threshold for the adaptive control of transmission packet size in 10th of percents, i.e. 1000 is 100.0%. Default: 10 (1%)

```
ascPacketSizeMaxFractionLost         OBJECT-TYPE ::= { ascConfig 12 }
```

Upper threshold for the adaptive control of transmission packet size in 10th of percents, i.e. 1000 is 100.0%. Default: 30 (3%)

```
ascJitterTotalFractionLostWeight     OBJECT-TYPE ::= { ascConfig 13 }
```

Factor for smoothing the varying fraction lost of incoming RTP packets caused by jitter in 10th of percents, i.e. 1000 is 100.0%. Default: 300 (30%)

```
ascJitterMinFractionLost             OBJECT-TYPE ::= { ascConfig 14 }
```

Lower threshold for the adaptive control of jitter buffer depth for incoming RTP packets in 10th of percents, i.e. 1000 is 100.0%. Default: 5 (0.5%)

```
ascJitterMaxFractionLost             OBJECT-TYPE ::= { ascConfig 15 }
```

Upper threshold for the adaptive control of jitter buffer depth for incoming RTP packets in 10th of percents, i.e. 1000 is 100.0%. Default: 40 (4%)

`ascJitterFactor                    OBJECT-TYPE ::= { ascConfig 16 }`

Factor for resizing the jitter buffer with respect to the average jitter: Default: 4

`ascJitterIncrement                 OBJECT-TYPE ::= { ascConfig 17 }`

Increment of jitter buffer if jitterMinFractionLost is exceeded in 100 microsecond steps: Default: 200 (20ms)

`ascJitterDecrement                 OBJECT-TYPE ::= { ascConfig 18 }`

Decrement of jitter buffer if smoothed average jitter falls below jitterMaxFractionLost in 100 microsecond steps: Default: 100 (10ms)

- **ASC DSP Config Group** (ascDspConfig) not relevant for IPDA components

`Implemented objects: { asc 3 }`

`dspIndex                              OBJECT-TYPE ::= { ascDspConfig 1}`

The index of the DSP channel to configure

`dspAgcLevel                           OBJECT-TYPE ::= { ascDspConfig 2}`

The target level to which the input signal will be scaled if AGC flag is enabled

`dspJitterBufferDepth                  OBJECT-TYPE ::= { ascDspConfig 6}`

The number of RTP packets in the jitter buffer. Set by host at the configuration time. To be set in multiples of 10 ms to a maximum of 210 ms

`dspJitterBufferAdaptationEnable       OBJECT-TYPE ::= { ascDspConfig 7}`

If this is set by host, the DSP jitter buffer adapts its depth based on its statistics. If not, host has to explicitly adjust the jitter buffer depth at run time based on statistics generated by the DSP

`dspRtpSenderNumEncodings              OBJECT-TYPE ::= { ascDspConfig 8}`

This has to be set in multiples of 10 ms for G.711 and in multiples of 30 ms for G.723

`dspAgcEnable                          OBJECT-TYPE ::= { ascDspConfig 9}`

Automatic Gain Control enable flag

`dspVadEnable                          OBJECT-TYPE ::= { ascDspConfig 10}`

The vad enable/disable flag to perform Voice Activity Detection. VAD is explicitly performed for G.711 only. Other speech coders perform VAD internally in their encoders

`dspEchoCancellerEnable                OBJECT-TYPE ::= { ascDspConfig 11}`

Echo canceller enable/disable ON/OFF flag

`dspDtmfEnable                         OBJECT-TYPE ::= { ascDspConfig 12}`

Specifies if dtmf tones are enabled

To make the ASC-MIB known to an MIB browser, the following files are required:

- smi_nbcs.my
- mibasc.my

These files are available in KMOSS (Knowledge Management for Operational Support and Service) under https://kmoss.icn.siemens.de.

Select **`KMOSS public`** and search for **`INF-05-000733`** in the **`Enterprise`** section.

Or click the following link:

https://kmoss.icn.siemens.de/livelink/llisapi.dll/view/INF-05-000733

20 IP Ports

20.1 General Information

The port assignments are available in the Interface Management Database (IFMDB):

https://apps.g-dms.com/ifm/

IP trunking + DMC (IP trunking and IPDA) master connections

The UDP port range is configured with the AMO CGWB for IP trunking master connections and DMC slave connections where HG 3500 is a DMC endpoint (i.e. for IP trunking or IPDA). The corresponding parameters are **UDPPRTLO** and **UDPPRTHI** in the branch **TYPE=ASC**.

The standard value for **UDPPRTLO** is 29100. **UDPPRTHI** is calculated based on the maximum number of B channels for the corresponding board.

Using DMC

- More ports are used that are managed by DNIL.
- Large board with five DSPs: maximum 100 channels (simultaneous MC/ DMC) --> a maximum of 400 ports (RTP/RTCP) are used.
- Small board with three DSPs: maximum 50 channels (simultaneous MC/ DMC) --> a maximum of 200 ports (RTP/RTCP) are used.

During operation, the board selects the ports from the configured value range of **UDPPRTLO** / **UDPPRTHI** for all features configured on a common gateway board.

IPDA (HG 3575/HG 3500) + DMC (HG 3575) master connections

- IPDA master connections

  The **UDPPORT** parameter in the AMO SIPCO is used for the payload stream in the IPDA master connection, i.e. for connections between the IPDA-HG 3500 and the HG 3575 and vice versa and for connections from HG 3575 to HG 3575.

  For IPDA master connections, only the start value is defined in the AMO SIPCO, **TYPE=DIFFSERV**, **UDPPORT=<4352 ... 65083>**. The upper value (=maximum number of ports actually used) is calculated on the basis of the number of B channels on the board used (multiplied by 2 because of RTCP).

  The port with the lowest value can be set to even values in the range [4352 ... 65280].

- DMC slave connections

The **UDPPORT** parameter in the AMO SIPCO applies similarly for DMC slave connections where NCUI2+/NCUI4 is the DMC endpoint. The following ports are automatically used.

Maximum port number for a board with 120 B channels:

With DMC:

up to 100 ports for the master connections + up to 100 ports for the associated DMC connections
=> 200 ports for the RTP and 200 ports for the RTCP stream

Without DMC:

up to 120 ports for the master connections
=> 120 ports for the RTP and 120 ports for the RTCP stream

An even port (such as 29000) is always selected for the RTP stream. The next odd port is selected for the appropriate RTCP port, i.e. RTCP port= RTP port +1.

IMPORTANT: The ports in use cannot be modified with the exception of ports for "UDP-Payload".

20.2 Examples

The following are a few examples to clarify the traffic restrictions applied to certain ports.

20.2.1 Payload

Depending on the board in use (HG 3500 or HG 3575), ports used are taken from a certain port range defined by the parameter UDPPORT (AMO SIPCO). The port range for RTP/RTCP is defined by the following interval: [UDPPORT .. UDPPORT + 247].

Port 4007 is used for a path test in the case of poor payload quality. See Section 4.8.1, “When is Payload Survivability Used?” in the document "IP Distributed Architecture (IPDA) and Access Point Emergency (APE)" - keyword "UDP-PINA".

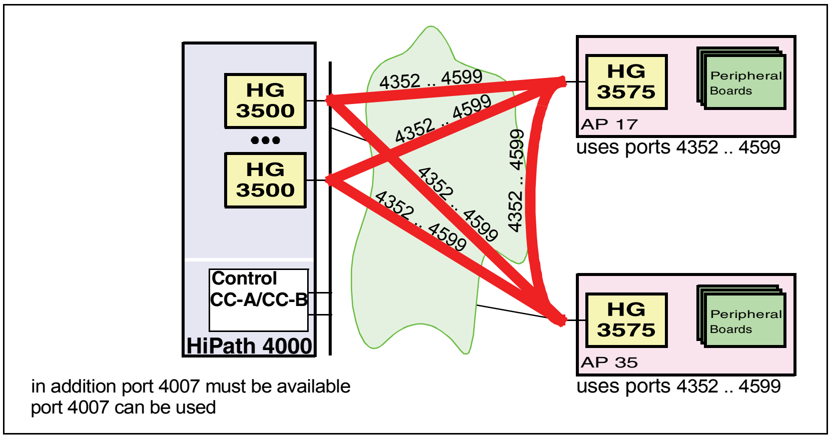


Figure 20 Example: Port usage for payload

20.2.2 Signaling

The term signaling refers to the entire data exchange between CC and access point. This includes loading and controlling peripheral boards, security messages, routine tests and naturally, all call processing messages including telephone display texts.

Every access point, that is, every HG 3575, has a signaling connection to the active CC.
The connection for this is always set up by the CM. The source port alternates between 1124 and 1125. The destination port (ASC HG 3575) is 4000.

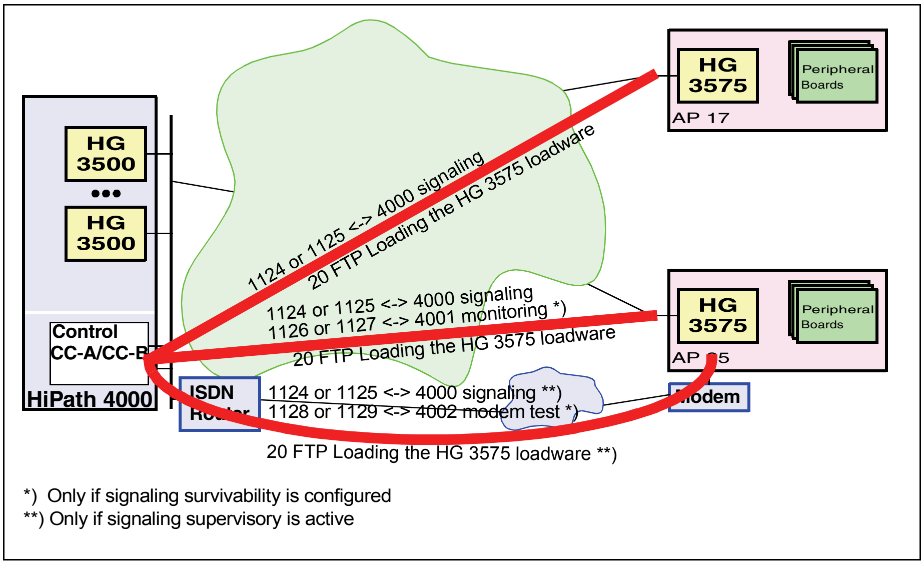
The HG 3575 loadware is loaded over FTP. The HG 3575 logs on to the CM’s FTP server for this. The FTP server grants read-only access to the HG 3575 configured and allows only one download at a time.

If signaling survivability is not configured (see Section 4.5, “Configuring Signaling Survivability” in the document "IP Distributed Architecture (IPDA) and Access Point Emergency (APE)"), additional connections are used.

The supervisory connection monitors the principal availability of the path from the CM to the HG 3575 in the IP network - in parallel to the signaling connection.
The connection for this is always set up by the CC. The source port alternates between 1126 and 1127. The destination port (ASC HG 3575) is 4001.

If the supervisory connection is interrupted, the signaling connection is re-routed over a PSTN router and modem. The signaling connection’s IP address and ports are retained.

The modem-based availability of a HG 3575 with signaling survivability is cyclically tested in normal mode.
The connection for this is always set up by the CM. The source port alternates between 1128 and 1129. The destination port (ASC HG 3575) is 4002.


HG 3500
•••
HG 3500
Control CC-A/CC-B
HiPath 4000
ISDN Router
HG 3575
Peripheral Boards
AP 17
HG 3575
Peripheral Boards
AP 35
Modem
1124 or 1125 <-> 4000 signaling
20 FTP Loading the HG 3575 loadware
1124 or 1125 <-> 4000 signaling
1126 or 1127 <-> 4001 monitoring *)
20 FTP Loading the HG 3575 loadware
1124 or 1125 <-> 4000 signaling **)
1128 or 1129 <-> 4002 modem test *)
20 FTP Loading the HG 3575 loadware **)

*) Only if signaling survivability is configured
**) Only if signaling supervisory is active

Figure 21 Example: Port usage for signaling

20.2.3 SNMP

The gateways HG 3500 and HG 3575 come with an SNMP agent which provides read-only access to MIB-2 data and a gateway-specific MIB. Please refer to Chapter 19, “SNMP Support HG 3500 / HG 3575”. Read-only access is supported. No parameters may be changed. No traps are transferred.

The SNMP agent waits by default at port 161.

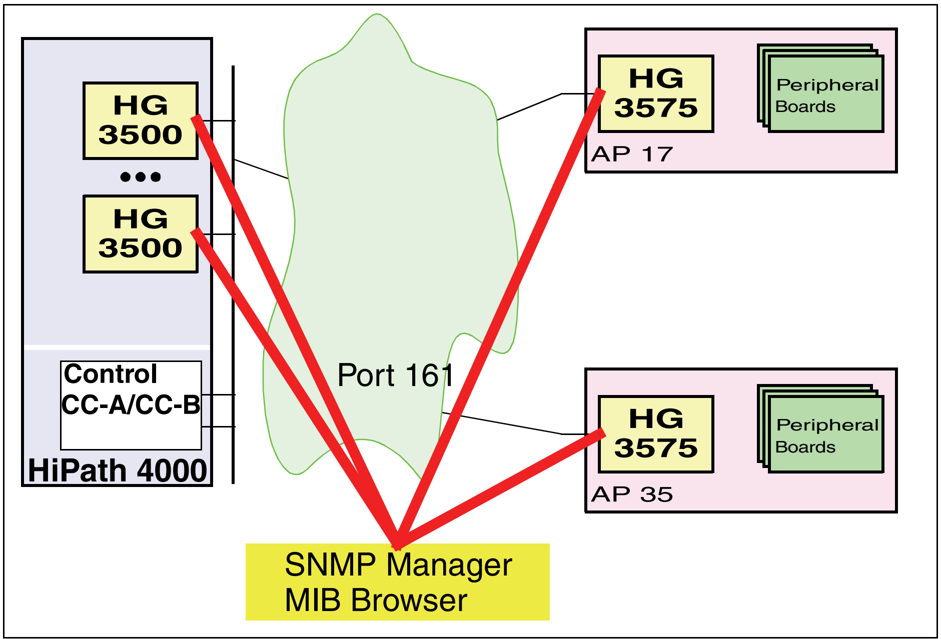


Figure 22 Example: Port usage for SNMP access

20.2.4 Diagnostics

Additional services that are normally inaccessible (ports blocked) can be activated on the gateways HG 3500 and HG 3575 for fault diagnosis.

These are

SSH	Port 22	TCP
HTTPS/WBM:	Port 443	Web server for accessing diagnostic data

Access can only be modified with the parameter FACCMODE (Facility Access Mode) in the DEBUG branch of the AMO STMIB (for HG 3575 only).

Logons with passwords can be configured to protect FTP- and TELNET-based access for the HG 3575. HG 3500 uses fixed values for this.

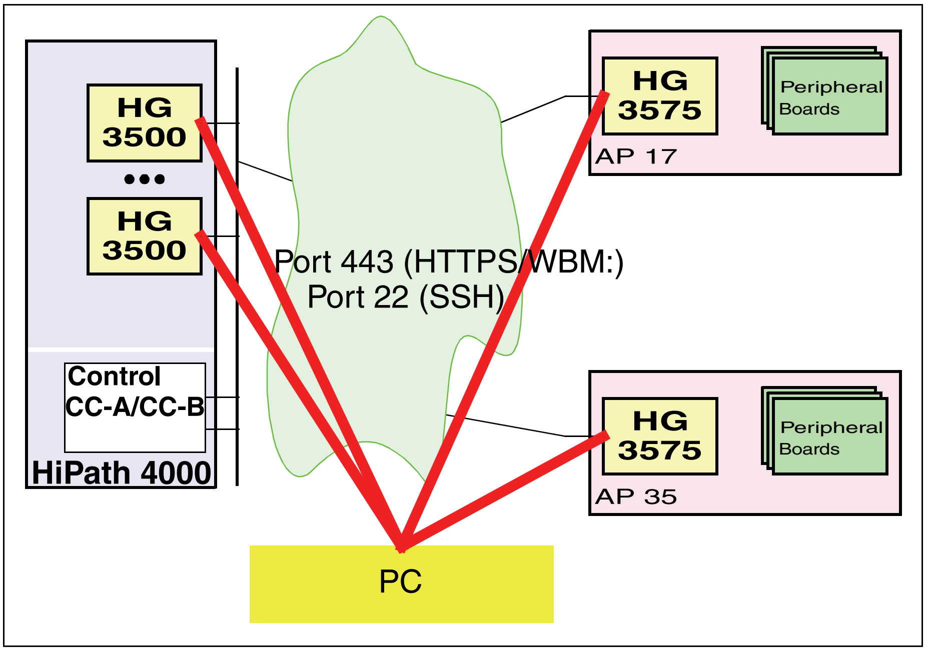


Figure 23 Example: Port usage for diagnosis

21 HG 3500 / HG 3575 Diagnostic Options

All diagnostic options for the gateways HG 3500 and HG 3575 are part of the WBM. The trace components can be configured in WBM. More information is provided in the WBM online help.

- Retrieving/deleting an event protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM

  Maintenance -> **Events** -> **Event Log** -> **Load via HTTP**

  Maintenance -> **Events** -> **Event Log** -> **Clear Event Log**

- Retrieving/deleting a trace protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM

  Maintenance -> **Traces** -> **Trace Log** -> **Load via HTTP**

  Maintenance -> **Traces** -> **Trace Log** -> **Clear Trace Log**

- Retrieving/deleting a customer trace protocol in the **T**rue **F**lash **F**ile **S**ystem (TFFS) via WBM.

  Maintenance -> **Traces** -> **Customer Trace Log** -> **Load via HTTP**

  Maintenance -> **Traces** -> **Customer Trace Log** -> **Clear Trace Log**

- V24 trace / console trace

- LAN trace for XTracer client

- Service center

- In the event of a system crash, the DDC log must be retrieved via WBM.

- Retrieving busy resources

22 Frequently asked Questions

4. **Question**: Are HG 3500 gateways supported on the Hicom 300 H?

   Answer: No. Customers have to upgrade to HiPath 4000 V4 or higher in order to take advantage of integrated IP gateways.

5. **Question**: Why does the HG 3500 require a static IP address?

   Answer: From an IP networking point of view the HG 3500 is a gateway/voice-router. Gateways/routers always require static IP addresses. This ensures that all IP devices always find their gateway/router without having to be reprogrammed constantly. Having dynamic IP addresses on gateways/routers does not make any practical sense.

6. **Question**: Is the HG 3500 supported on IP distributed Access Points?

   Answer: Yes. The HG 3500 version is supported on IP distributed Access Points. Excessive delays that resulted from multiple TDM to IP conversions when IP users on the IP Access Points call IP users on other IP Access Points or IP users on the host are eliminated using DMCs.

7. **Question:** Why do HG 3500 and HG 3575 not support DHCP?

   Answer: Consider HG 3500/3575 as a voice router. These voice routers must always be available and know each other.
   As is the case with IP router ports, it is useful to work with fixed IP addresses. For complete system availability, it is also better to avoid dependencies on DHCP and/or DNS servers.

8. **Question**: Why does the HG 3500 not support the G.722 codec?

   Answer: There is absolutely no need for the HG 3500 to support G.722 because there is no wideband quality available on the TDM side; G.722 strictly works between IP clients and it is the clients that negotiate the codec type. The HG 3500 will pass the signaling between any IP clients that support G.722, enabling high quality voice.

9. **Question:** Why is the default value for the jitter buffer set to 60 milliseconds on HG 3500/75? Can lower values also be set without leading to problems?

   Answer: The default setting should ensure that initial startup runs relatively smoothly. 60 ms is definitely too high for modern campus LAN installations that only use device connections at Layer-2 switch ports and have sufficient bandwidth reserves. A jitter buffer depth of 20 ms has been shown to be satisfactory.
   On the other hand, 60 ms may sometimes be too low for installations over WAN links with extremely low bandwidth and no reserve.
   Setting the jitter buffer depth too high causes an unnecessarily high voice delay. Setting it too low leads to poor transmission quality as a result of high packet loss rates. This poses problems particularly for fax, modem, and ISDN data connections.

10. **Question:** The maximum value that can be set for the jitter buffer is 210 ms. I assume that the system works properly with this setting. Can I specify this value in my WAN tender specification as a carrier requirement?

    Answer: The system has no problems with a 210 ms jitter buffer. This setting can balance out an extremely high jitter value of up to 210 ms without impairing voice comprehension. It should be noted, however, that the size of the jitter buffer has a direct effect on voice delay. See also Section 2.4, "Voice Quality". Voice delay (mouth-to-ear delay) is influenced by five elements:

    - Packet size/sample size/the number of audio milliseconds per packet
    - Processing time on the receiving end
    - Transmission time in the LAN/WAN
    - Jitter buffer
    - Processing time on the receiving end

    Figure 4 Voice quality depending on delay illustrates user satisfaction in relation to the mouth-to-ear delay. Satisfaction drops dramatically at around 150 ms. Users start to notice interference at around 250 ms and become dissatisfied.

    Please note that a similar installation can also cause delays in trunk calls at the other end of the CO trunk. In other words, only one half of the tolerable delays may be caused by each end.

    The following table shows a couple of sample calculations (all values in ms)

Sample size	20	60	20	20	60	60	60	20
Transmission time in the LAN/ WAN	10	10	10	40	40	40	60	0
Processing time Send+receive direction	32	32	32	32	32	32	32	32
Jitter buffer	20	20	60	60	60	120	**210**	**210**
Mouth-to-ear delay	82	122	122	152	192	252	**362**	**262**

    It is not possible to achieve delays under 262 ms with a 210 ms jitter buffer.

11. **Question:** Both the HG 3500 and the HG 3575 have a fixed MAC address for the Ethernet port assigned to the board. The IP addresses, however, are assigned from the system database on the basis of the board's "PEN". If I switch a HG 3500 in a particular slot with another board of the same type, the IP address is maintained from the IP network's perspective. However, the MAC address to which the packets are sent changes. Doesn't this mean that the new board cannot be reached on account of the modified MAC address until *aging* makes the ARP entries obsolete in the IP stacks?

Answer: The standard solution for this problem which is principally an address resolution issue is also implemented on the HG 3500 and HG 3575 gateways. After activating the hardware interface, the gateway sends an ARP request “gratuitous ARP“ to the actual IP address. This way, all IP devices on the LAN segment learn the new IP <-> MAC address assignment.

12. **Question:** We regularly encounter statistic overflow problems in a customer installation. Individual HG 3500/75 boards are temporarily taken out of service. This clears down all calls over these boards but does not have any other visible effect. What causes this problem and what can be done about it?

Answer: A statistical evaluation of error messages is performed for the HG 3500/75 in the same way as for other boards. This also includes the loss of the signaling connection in HG 3575 and “bad quality“ messages for the HG 3500/75 payload connections.

Poor IP connection quality between the HG 3500/75 gateways or the HiPath 4000 central system and the HG 3575 over a sustained period can lead to a large number of error messages in a short space of time, which in the end causes a statistic overflow and a board reset.

Resetting the board should prevent a temporary board fault from turning into a problem.

If the fault clearly originates in the network, no improvements will be achieved by resetting the board.

You can use the AMO PSTAT to increase the threshold values for the STMI and NCUI counters or deactivate the statistical evaluation entirely by setting the threshold values to zero.

```
CHANGE-PSTAT:TYPE=CTRLTAB,LEVEL=BOARD,BOARD=NCUI,FAULT=1 or 2,
MAXCOUNT=xxx;
```

Stage 1 (`COUNT1`, counts pairs of in-service and out-of-service messages) and stage 2 (`COUNT2`, counts messages that could develop into a message flood) should also be taken into consideration.

Separate counters are used for NCUI/STMI and NCUI2/STMI2

```
+----------+--------+----------+----------+----------+----------+----------+
! NCUI     ! COUNT1 !   Byte1  !     61   !     10   !      2   !      4   !
! STMI     +--------+----------+----------+----------+----------+----------+
!          ! COUNT2 !   Byte2  !     61   !      6   !      2   !      2   !
!          +--------+----------+----------+----------+----------+----------+
!          ! COUNT3 !   Byte3  !     21   !      10   !      2   !      4   !
!          +--------+----------+----------+----------+----------+----------+
!          ! COUNT4 !   Byte4  !     19   !      10   !      2   !      4   !
+----------+--------+----------+----------+----------+----------+----------+
! NCUI2    ! COUNT1 !   BYTE1  !    241   !     10   !      2   !      4   !
! STMI2     +--------+----------+----------+----------+----------+----------+
!          ! COUNT2 !   Byte2  !     241   !      6   !      2   !      2   !
!          +--------+----------+----------+----------+----------+----------+
!          ! COUNT3 !   Byte3  !     21   !      10   !      2   !      4   !
!          +--------+----------+----------+----------+----------+----------+
!          ! COUNT4 !  Byte4   !     19   !     10   !     2    !     4    !
+----------+--------+----------+----------+----------+----------+----------+
```

Details on the AMO PSTAT can be found in the AMO description in the HiPath 4000 Service Manual.

Modifying the statistics prevents the boards from being reset when quality problems that affect the overall function of the system occur in the IP network. Your objective must be get these problems under control.

13. **Question:** Where can I hear how packet loss concealment affects the G.711 or G.729 codec?

    The suggestion to provide acoustic samples in the electronic version of the handbook was rejected by Service and Sales because this information is not relevant for service technicians and sales managers. Sorry!

Index