TELES.MANUALS

TELES.iGATE

Software version 14.0

TELES Communication Systems

TELES AG
Communication Systems Division
Ernst-Reuter-Platz 8
10587 Berlin, Germany
Phone: +49 30 399 28-00
Fax: +49 30 399 28-01
E-mail: sales@teles.com

http://www.teles.com/tcs/

Software version: 14.0. Revised: 12 June 2008.

All text and figures in this publication have been compiled with great attention to detail. Nonetheless, inaccuracies and typographical errors cannot be entirely avoided. TELES AG Informationstechnologien provides this document 'as is' without warranty of any kind, expressed or implied. TELES AG Informationstechnologien reserves the right to make changes in product design or specifications without notice.

Chapter 1 – About this Manual 9
1.1 organization 9
1.2 conventions. 9
1.3 Safety Symbols 10

Chapter 2 – Safety and Security Precautions. 11
2.1 Safety Measures 11
2.2 FCC / Industry Canada Notice 11
2.3 Tips for EMC Protection. 12
2.4 System Security 12
2.5 Servicing the System 13
2.5.1 Replacing Components 13
2.5.2 Protecting the Operating System 13
2.6 CDR Files 14
2.7 Network Security. 14

Chapter 3 – Overview 17
3.1 What's New in Version 14.0 18
3.2 Features. 19
3.3 How iGATE Works 20
3.4 Supported Implementation Scenarios 20

Chapter 4 – Installation 23
4.1 Checklist 23
4.2 Package Contents 23
4.3 Hardware Description 23
4.4 Installation Requirements 25
4.4.1 Ethernet Wiring 25
4.4.2 PRI Wiring 26
TELES to TBR12 26
Former TELES Assignment to Current TELES Assignment 26
4.4.3 BRI Wiring 27
4.4.4 Antenna Connection. 27
4.4.5 SIM Cards. 27
The SIM-Card Carrier Module 28
4.5 Preparing for Installation. 31
4.6 Hardware Connection 31
4.7 Startup with Quickstart 31
4.7.1 Installing Quickstart 32
4.7.2 Configuration with Quickstart 33
4.8 Startup via FTP 34
4.9 Self Provisioning with NMS 35

4.10 LED Functionality. 35
4.10.1 iLCR Base Board PRI Port LEDs 35
4.10.2 iGATE 4 Mobile Board SIM-Card LEDs. 36
4.11 Remote Access and Access Security 37
4.11.1 GATE Manager 38
4.11.2 FTP. 39
4.11.3 Setting a Password for Remote Access 40

Chapter 5 – Configuration Files 41

5.1 Configuration File ip.cfg 42
5.1.1 System Section Configuration 43
5.1.2 Ethernet Interface Configuration 43
5.1.3 Bridge Configuration 44
5.1.4 NAT Configuration 44
5.1.5 PPPoE Configuration. 46
5.1.6 Firewall Settings 46
5.1.7 Bandwidth Control 48
5.1.8 DHCP Server Settings 50
5.1.9 PPP Configuration for ISDN and CDMA Dial-Up. 51
5.1.10 VLAN Configuration 53
5.1.11 Examples 53
Default Configuration 53
Active Ethernet Bridge 53
Integrated DSL-Router Scenario for VoIP Traffic with an Active DHCP Server and Firewall. 55
VLAN Scenario 56
5.2 Configuration File pabx.cfg 56
5.2.1 System Settings 56
Life Line 56
Log Files. 57
Night Configuration 59
Controllers 60
Subscribers. 64
Global Settings. 68
5.2.2 SMTP-Client Configuration 72
5.2.3 Number Portability Settings. 74
5.2.4 SNMP Settings 75
5.2.5 Time-Controlled Configuration Settings. 75
5.2.6 .CAS R2 Settings 75
5.3 Configuration File route.cfg. 76

5.3.1 Entries in the [System] Section 76
Mapping 77
Restrict. 78
Redirect 79
Setting the Time-Controlled Sections. 81
5.3.2 VoIP Profiles. 82
5.3.3 Gatekeeper Profiles 85
5.3.4 Registrar Profiles 87
5.3.5 Radius Profiles 88

Chapter 6 – Routing Examples. 90

6.1 iGATE Integration in a Carrier Network. 90
6.2 iGATE Integration with SIM-Card Switching in an H.323 Carrier Network 91
6.3 iGATE as a Second-Generation LCR with VoIP 93

Chapter 7 – Mobile Configuration Options 95

7.1 Connection to a vGATE 95
7.2 Module Distribution of Various Mobile Networks 95
7.3 Network-Specific Mobile Routing 97
7.3.1 Using a Fixed Mobile Port Address 97
7.3.2 Using the LAIN as the Mobile Port Address 98
7.3.3 Fixed LAIN for a Mobile Port 99
7.4 Incoming Voice Calls from Mobile. 99
7.5 Blocking Ports 99
7.6 Setting Limits. 100
7.7 Automatic SIM Switching 101
7.7.1 Switching SIMs. 102
7.7.2 Cyclical SIM Switching 102
7.7.3 Immediate SIM Switching 102
7.7.4 Count Status Information 102
7.8 Defining Time Limits for Calls 103
7.9 Pause between Two Calls 104
7.10 Time-Controlled SIM Switching 104
7.11 Mobile-User PBX Callback. 106
7.12 Optional Mobile Quality Parameters 107
7.13 Deactivating Class 2 Re-Routing 108
7.14 Checking Ports/Mobile Channels. 108
7.15 Recharging Prepaid SIMs. 109
7.15.1 Recharge Preparation 110
Checking the Active SIM 110
Addressing SIMs Using Port- and Controller-Specific Routing. 110
Blocking the Port Containing the Recharging SIM 111

7.15.2 Recharging Procedure 111
Direct Recharging via Call 111
Indirect Recharging via GATE Manager 112
7.15.3 Prepaid Account Status Query 117
Direct Account-Status Query 117
Indirect Account-Status Query 117
Saving /Forwarding the Account Status 118
7.16 Defining Special Characters for Voice Calls 118

Chapter 8 – Signaling and Routing Features 119

8.1 Digit Collection (Enblock/Overlap Receiving) 119
8.2 Rejecting Data Calls and Specified Numbers 119
8.2.1 Blacklist Routing 119
8.2.2 Whitelist Routing 120
8.2.3 Rejecting Calls with ISDN Bearer Capability Data 120
8.2.4 Specific Routing of Data Calls via VoIP 121
8.3 CLIP and CLIR 121
8.3.1 Routing CLIP and CLIR Calls 121
8.4 Routing Calls without CLIR 122
8.4.1 Setting CLIR 122
8.4.2 Setting CLIP 122
8.5 Conversion of Call Numbers 123
8.6 Setting Number Type in OAD/DAD 123
8.7 Setting the Screening Indicator 125
8.8 Setting a Default OAD 125
8.9 Setting or Removing **Sending Complete** Byte in Setup 126
8.10 Miscellaneous Routing Methods 127
8.10.1 Routing Calls without a Destination Number 127
8.10.2 Routing Calls Based on an Extension Prefix or on the Length of the Destination Number 127
8.11 Changing Cause Values 128

Chapter 9 – Additional VoIP Parameters 130

9.1 Signaling Parameters 130
9.2 Registrar Parameters 135
9.3 Routing Parameters 137
9.4 Quality Parameters 138
9.5 Compression Parameters 145
9.6 Fax/Modem Parameters 146
9.7 DTMF Parameters 148

Chapter 10 – System Maintenance and Software Update 149

10.1 Configuration Errors 149

10.2 Status and Error Messages 149
10.3 Software Update 156
10.4 Trace 158
10.4.1 ISDN Trace Output 160
10.4.2 GSM/CDMA/UMTS Trace Output. 160
10.4.3 VoIP Trace Output 161
Interface IP Network. 162
Internal Protocol Interface (to ISDN, Mobile) 173
H.245 Messages. 175
RAS (Registration, Admission, Status) 180
ENUM Output. 185
Examples 185
10.4.4 Remote Output. 189
10.4.5 SMTP Trace Output. 190
10.4.6 Number Portability Trace Output. 193
10.4.7 DTMF Tone Trace Output 194

Chapter 11 – Feature Packages 197

11.1 Activating the License 197
11.2 DLA/Callback Server Functionality. 198
11.2.1 Call Connector and Callback Server. 198
Special Announcement 199
DLA with DTMF 199
DLA with Fixed Destination Number 199
Callback with DTMF and OAD as Callback Number 200
Callback with DTMF and Pre-Configured Callback Number 200
Callback to OAD and Fixed Second Leg 201
DLA with DTMF and PIN for First Leg and Callback for Second Leg 201
Using a PIN in Front of the Call Number 202
11.3 Least Cost Routing 202
11.3.1 Carrier Selection 203
Routing Entries. 203
11.3.2 Alternative Routing Settings 204
11.3.3 Charge Models. 204
11.3.4 Generating Charges with the iGATE 206
11.4 Online Traffic Monitor 208
11.4.1 ASR Calculation and Resetting Statistic Values 208
11.4.2 Generating and Retrieving CDRs 209
Call Log 210
Missed Calls List. 213
Sending CDRs via E-Mail. 214
11.5 SMS Gateway 214

11.5.1 Sending SMS via E-mail . . . 214
11.5.2 Receiving SMS Messages . . . 215
SMS to E-Mail . . . 215
SMS to SMS . . . 216
SMS to File . . . 216
11.5.3 Incoming USSD (Unstructured Supplementary Services Data) . . . 216
11.5.4 Sending Messages via E-mail . . . 217
11.5.5 Setting Up Connections via E-Mail . . . 217
11.5.6 Sending Anouncements via E-Mail . . . 218
11.5.7 Displaying Incoming Calls . . . 218
11.5.8 Sending Automatic SMS for Unconnected Calls . . . 218
11.6 Ported Number Screening . . . 219
11.6.1 System Requirements . . . 220
11.6.2 Routing and Configuration . . . 220
11.7 SS7-Specific Settings . . . 221
11.7.1 General SS7 Terminology . . . 221
11.7.2 What is SS7? . . . 222
11.7.3 Signaling Types. . . . 222
Associated Signaling. . . . 222
Quasi-Associated Signaling . . . 222
11.7.4 Signaling Points . . . 222
Signaling End Points . . . 223
Signaling Transfer Points. . . . 223
Service Control Points . . . 223
11.7.5 SS7 Protocol Stack . . . 224
Message Transfer Part . . . 224
ISDN User Part . . . 225
Telephone User Part . . . 225
Signaling Connection Control Part. . . . 225
Transaction Capabilities Application Part. . . . 225
Operations, Maintenance and Administration Part. . . . 225
Mobile Application Part . . . 225
Intelligent Network Application Protocol . . . 226
11.7.6 SS7 and the iGATE . . . 226
11.7.7 SS7 Routing Entries . . . 228

Chapter 12 – Optional Function Modules . . . 230

12.1 Overview . . . 230
12.2 SNMP Agent . . . 230
12.3 DNS Forwarder . . . 231
12.4 ipupdate - DynDNS Client . . . 232

1 ABOUT THIS MANUAL

Congratulations on the purchase of your new iGATE! This manual is set up to guide you through the step-by-step installation of your iGATE, so that you can follow it through from the front to the back. Quick-installation instructions appear in Chapter 4.7, "Startup with Quickstart" ⇨.

Make sure you familiarize yourself thoroughly with the safety and security precautions detailed in Chapter 2 ⇨ before you begin to install your iGATE. TELES is not liable for any damage or injury resulting from a failure to follow these safety and security instructions!

1.1 ORGANIZATION

This manual is organized into the following chapters.

Chapter 1, "About this Manual" ⇨ introduces the iGATE Systems Manual and how it is set up.

Chapter 2, "Safety and Security Precautions" ⇨ contains information about security issues relevant to connection with the IP network.

Chapter 3, "Overview" ⇨ briefly describes the iGATE and its implementation scenarios.

Chapter 4, "Installation" ⇨ contains information on how to connect and configure the system so that it is ready for operation.

Chapter 5, "Configuration Files" ⇨ describes the iGATE's individual configuration files and parameters.

Chapter 6, "Routing Examples" ⇨ contains useful examples and descriptions of scenario-based configurations in the `route.cfg`.

Chapter 7, "Mobile Configuration Options" ⇨ describes mobile configuration entries.

Chapter 8, "Signaling and Routing Features" ⇨ describes configuration settings in the `route.cfg` used for adjusting PRI signaling and customizing the configuration for specific scenarios.

Chapter 9, "Additional VoIP Parameters" ⇨ contains additional configuration entries to fine-tune communication with the VoIP peer.

Chapter 10, "System Maintenance and Software Update" ⇨ describes system messages that are saved in the protocol file, as well as trace options.

Chapter 11, "Feature Packages" ⇨ contains a description of options that expand the iGATE's functionality.

Chapter 12, "Optional Function Modules" ⇨ contains a description of expansion modules.

1.2 CONVENTIONS

This document uses the following typographic conventions:

- **Bold** – items from the GUI menu.
- Halfbold – items from the GUI and the menu.
- `Code` – file names, variables and constants in configuration files or commands in body text.
- "conventions" on page 9 ⇨ – cross-references can be accessed in the PDF files by a single mouse click.

Configuration data or extracts are written in single-column tables with a gray background.

1.3 SAFETY SYMBOLS

The following symbols are used to indicate important information and to describe levels of possible danger.

ⓘ	**Note** **Useful information with no safety implications.**
⚠	**Attention** **Information that must be adhered to as it is necessary to ensure that the system functions correctly and to avoid material damage.**
⚠	**Warning** **Danger. Could cause personal injury or damage to the system.**
⚡	**Dangerous voltage** **Could cause injury by high voltage and/or damage the system.**
⚠	**Electrostatic discharge** **Components at risk of discharge must be grounded before being touched.**

2 SAFETY AND SECURITY PRECAUTIONS

Please be sure and take time to read this section to ensure your personal safety and proper operation of your TELES Infrastructure System.

To avoid personal injury or damage to the system, please follow all safety instructions before you begin working on your TELES Infrastructure System.

TELES Infrastructure Systems are CE certified and fulfill all relevant security requirements. The manufacturer assumes no liability for consequential damages or for damages resulting from unauthorized changes.

This chapter applies for all Access Gateways. Information that applies only for individual Access Gateways specifies the system for which it applies.

2.1 SAFETY MEASURES

Danger of electric shock - the power supplies run on 230 V. Unplug the TELES Infrastructure System from its power source before working on the power supply or extension socket.
Bear in mind that telephone and WAN lines are also energized and can cause electric shocks.
Do not insert foreign objects into openings in the device. Conductible objects can cause short circuits that result in fire, electric shock or damage to the device.
Do not open the TELES Infrastructure System except to install an additional TELES.Component. Changes in the device are not permitted.

Make sure to install the system near the power source and that the power source is easily accessible.
Wire your system using only the cables included in the package contents. Use only proper ISDN and Ethernet cables.
Be sure to respect country-specific regulations, standards or guidelines for accident prevention.

2.2 FCC / INDUSTRY CANADA NOTICE

The following information applies for the iGATE GSM only.

In accordance with the manufacturer’s specifications, the iGATE comes installed with modular transmitters Q24CL001 (FCC ID: O9EQ24CL001) and Q24PL001 (FCC ID: O9EQ24PL001).

The antenna gain, including cable loss, must not exceed 3 dBi at 1900 MHz / 1.4 dBi at 850 MHz for mobile operating configurations and 7 dBi at 1900 MHz / 1.4 dBi at 850 MHz for fixed mounted operations, as defined in 2.1091 and 1.1307 of the rules for satisfying RF exposure compliance.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.

The iGATE has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2.3 TIPS FOR EMC PROTECTION

Use shielded cables.
Do not remove any housing components. They provide EMC protection.

2.4 SYSTEM SECURITY

This section describes all points crucial to the TELES Infrastructure System’s system security.

The system’s location must support normal operation of TELES Infrastructure Systems according to EN ETS 300 386. Be sure to select the location with the following conditions in mind:

Location: Make sure you install the system horizontally in a clean, dry, dust-free location. If possible, the site should be air-conditioned. The site must be free of strong electrical or magnetic fields, which cause disrupted signals and, in extreme cases, system failure.

Temperature: The site must maintain a temperature between 0 and 45°C. Be sure to guard against temperature fluctuations. Resulting condensation can cause short circuiting. The humidity level may not exceed 80%.
To avoid overheating the system, make sure the site provides adequate ventilation.

Power: The site must contain a central emergency switch for the entire power source. The site's fuses must be calculated to provide adequate system security. The electrical facilities must comply with applicable regulations.

The operating voltage and frequency may not exceed or fall below what is stated on the label.

Antenna: iGATE contains no provision or protective device against power surges or lightning strikes.

The installation of the antenna must fulfill all necessary safety requirements. Employ the services of a professional antenna installer.

2.5 SERVICING THE SYSTEM

Regular servicing ensures that your TELES.System runs trouble-free. Servicing also includes looking after the room in which the system is set up. Ensure that the air-conditioning and its filter system are regularly checked and that the premises are cleaned on a regular basis.

2.5.1 REPLACING COMPONENTS

If your system contains any of the following components, replace them according to the following table:

Table 2.1 Component Life Span

Component	Life span
Filter pads	6 months
Power adapter	5 years
Fan	5 years

2.5.2 PROTECTING THE OPERATING SYSTEM

Changing configuration data and/or SIM card positions may lead to malfunctions and/or misrouting, as well as possible consequential damage. Make changes at your own risk. TELES is not liable for any possible damage resulting from or in relation to such changes. Please thoroughly check any changes you or a third party have made to your configuration!

Make sure your hard disk or flash disk contains enough storage space. Downloading the log files and deleting them from the system on a regular basis will ensure your system's reliability.

Be careful when deleting files that you do not delete any files necessary for system operation.

⚠ **TELES.vGATE Control Unit:**
Do not use Ctrl/Alt/Del (Task Manager) to shut down vGateDesktop or vGateCtrl. Do not perform queries on the database. This can result in damages to the database. Do not use any MySQL tools, such as MySQL-Front to make changes in or perform tests on the database.

2.6 CDR FILES

Call Detail Records are intended for analysis of the system's activity only. They are not designed to be used for billing purposes, as it may occur that the times they record are not exact.

ⓘ **Inaccuracies in the generation of CDRs may occur for active connections if traffic is flowing on the system while modifications in configuration or routing files are activated.**

2.7 NETWORK SECURITY

Every day hackers develop new ways to break into systems through the Internet. While TELES takes great care to ensure the security of its systems, any system with access through the Internet is only as secure as its user makes it. Therefore, to avoid unwanted security breaches and resulting system malfunctions, you must take the following steps to secure your TELES.System if you connect it to the Internet:

- Use an application gateway or a packet firewall.
- To limit access to the system to secure remote devices, delete the default route and add individual secure network segments.
- Access to the system via Telnet, FTP, HTTP, GATE Manager or remote vGateDesktop must be password protected. Do not use obvious passwords (anything from `sesame` to your mother-in-laws maiden name). Remember: the password that is easiest to remember is also likely to be easiest to crack.

The firewall must support the following features:

- Protection against IP spoofing
- Logging of all attempts to access the system

The firewall must be able to check the following information and only allow trusted users to access the TELES.System:

- IP source address
- IP destination address
- Protocol (whether the packet is TCP, UDP, or ICMP)
- TCP or UDP source port
- TCP or UDP destination port
- ICMP message type

For operation and remote administration of your TELES.System, open only the following ports only when the indicated services are used:

Table 2.2 Default Ports Used for Specific Services

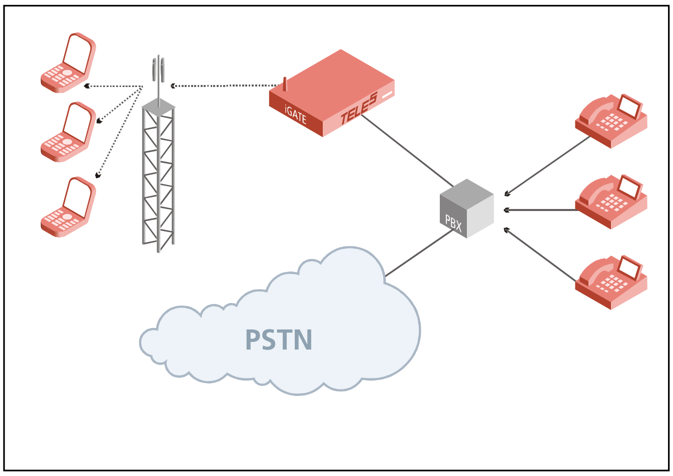
Service	Protocol	Port
For all systems except vGATE		
FTP	TCP	21 (default, can be set)
Telnet (for TELES debug access only)	TCP	23
SMTP	TCP	25
DNS forward	UDP	53
HTTP	TCP	80 (default, can be set)
SNTP	UDP	123
SNMP	UDP	161
H.225 registration, admission, status	UDP	1719 (default, can be set)
H.225 signaling	TCP	1720 (default, can be set)
Radius	UDP	1812 (default, can be set)
Radius accounting	UDP	1813 (default, can be set)
GATE Manager	TCP	4445 (default, can be set)
SIP signaling	UDP / TCP	5060 (default, can be set)
RTP	UDP	29000-29120 (default, can be set)
TELES.vGATE Control Unit	TCP	57343
vGATE tunneling	TCP	4446
For TELES.vGATE Control Unit and iMNP		
FTP	TCP	21
Telnet	TCP	23
MySQL database	TCP	3306
iGATE or TELES.VoIPBOX GSM/CDMA 4FX to vGATE	TCP	57342
vGATE tunneling to iGATE or TELES.VoIPBOX GSM/CDMA 4FX	TCP	4446

Table 2.2 Default Ports Used for Specific Services *(continued)*

Service	Protocol	Port
iGATE **or** TELES.VoIPBOX GSM/ CDMA 4FX to iMNP	TCP	9003
Remote vGateDesktop	TCP	57344
Remote vGateDesktop (read only)	TCP	57345
iMNP	TCP	9003
For vGATE Sim Unit		
TELES.vGATE Control Unit plus iGATE **or** TELES.VoIPBOX GSM/ CDMA 4FX	TCP	51500
For NMS		
FTP	TCP	21
Telnet	TCP	23
MySQL database	TCP	3306
NMS protocol	TCP	5000
NMS update	TCP	5001
NMS task	TCP	5002
NMS task	TCP	5003
NMS Listen	TCP	4444
For vGATE Call Manager		
Radius authentication	UDP	1812
Radius accounting	UDP	1813

Connection from a TELES.vGATE Control Unit to a iGATE requires ICMP access. The TCP filters listed above are activated in the default configuration of the TELES.vGATE Control Unit or the NMS server.

3 OVERVIEW



Mobile phone charges have become an important cost factor for many carriers and companies. Connections from the fixed network to mobile networks share a considerable amount of these costs.

The iGATE can help reduce these costs up to 70%, because calls from mobile network to mobile network cost significantly less than calls from the fixed network to mobile networks. Fixed-to-mobile calls that travel through the iGATE are routed and billed as if they occurred within the same mobile network. You can insert SIM cards from any carrier into the SIM4 or SIM24 module.

Depending on whether your system includes iGATE 4 GSM Boards, iGATE 4 CDMA Boards or iGATE 4 UMTS Boards, each iGATE can provide direct access to the GSM, CDMA or UMTS mobile network with up to 32 mobile channels – 4 mobile channels per iGATE 4 Mobile Board or up to 8 iGATE 4 Mobile Boards per iGATE. The TELES.iGATE Antenna Splitter Board combines the antennas so that only one or two antennas leave the system.

The iGATE has 2 optional PRI ports, optional BRI ports and VoIP functionality, which provides up to 32 VoIP channels, so connection of the mobile gateway occurs by VoIP. The iGATE combines the cost savings resulting from implementation of the iGATE with those of Voice over IP transmission. iGATEs can be set up in various national or international locations.

The iGATE features packages are modular expansion applications that provide services in addition to those offered with the standard software. Feature packages can be activated separately or in combination with one another, so that you can design your system according to your own needs.

The iGATE supports all of the following standards:

- GSM (Global System for Mobile Communications)
- CDMA (Code-Division Multiple Access)
- UMTS (Universal Mobile Telecommunications System)

Throughout this manual, the following boards will be referred to as iGATE 4 Mobile Board, unless otherwise specified:

- iGATE 4 GSM Board
- iGATE 4 CDMA Board
- iGATE 4 UMTS Board

3.1 WHAT'S NEW IN VERSION 14.0

- Enhanced HTTP user interface
- Supports the CAS R2 protocol
- Supports the NI2 protocol
- Supports the T1 line type
- Possible to configure individual mobile bands
- LAIN can now contain up to six digits
- Supports PPP dialup via UMTS
- New SIP settings:
  - VoipSdpProxy=<mode>: enables transmission of all SDP parameters if a call is from SIP to SIP
  - VoipUseRad=<mode>: different addresses in request header and To field result in redirected ISDN number
  - Customized translation of DSS1 cause values to SIP events
- Supports 3G faxes
- Configurable time interval for echo detection in VoIP
- New configuration settings for VoIP DTMF tone handling
- Radius accounting request contains SIM's IMSI to enable SIM-specific billing
- Expanded functionality of integrated DLA/callback server
- Integrated mail client capable of SMTP authentication
- CDR enhancement with new output for VoIP calls (codec, ptime)

3.2 FEATURES

- Easy installation with Quickstart
- Conversion of PRI (optional) or VoIP to up to 32 mobile channels and vice versa
- Requires only two antennas for 32 mobile channels with TELES.iGATE Antenna Splitter Board
- Centralized SIM management with vGATE
- Call distribution/rerouting of temporarily unavailable mobile channels
- Automatic use (configurable) of the defined SIM cards per mobile channel
- Enblock and overlap receiving
- Conversion of call numbers
- Inband tone detection
- Can block specified telephone numbers and services
- Summarizes reject causes based on definable cause values
- Remote administration via Ethernet or ISDN
- Online monitoring, management and configuration via GATE Manager and NMS (Network Management System)
- Generates CDRs and transmits online CDRs (optional)
- Time-controlled configuration (optional)
- Built-in cutting edge LCR: Full-featured TELES least cost routing between PBX and PSTN (optional)
- Optional 24 SIM-card carrier can handle up to 24 SIM cards on 4 mobile channels; SIMs can be randomly distributed at will (optional)
- Callback function supported (optional)
- Direct Line Access function (optional)
- Number Portability (optional)
- International SS7: Q.767 (optional)
- PPP client/server mode

VoIP

- Modular 16 to 180 channels
- H.323 v.4 / SIP v.2 signaling (RFC 3261), operating in parallel
- Various audio codecs: G.711, G.723.1, G.726, G.728, G.729, GSM, iLBC, Fax T.38, Data: clear channel
- Gatekeeper support
- Registrar support
- RTP multiplexing
- STUN (support for non-static IP addresses)
- ENUM (changes phone numbers into IP addresses)

3.3 HOW IGATE WORKS

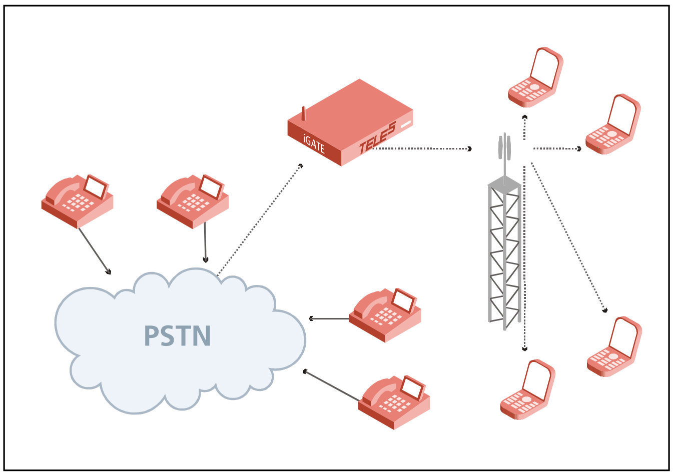
The iGATE is connected to the PSTN or an IP network and to the mobile network.

- During outgoing calls from the PSTN or IP network to mobile, dialed digits are compared with the routing-table entries for various mobile networks. The calls are then routed through the corresponding SIMs in the iGATE and forwarded to the number dialed.
- Only the connection from the SIM in the iGATE to the mobile number in the same mobile network is charged.

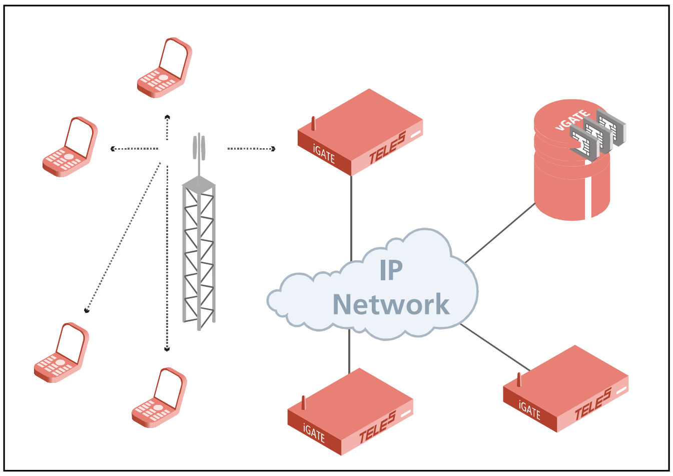
3.4 SUPPORTED IMPLEMENTATION SCENARIOS

In each of the following scenarios, calls are routed through individual gateways into the mobile network:

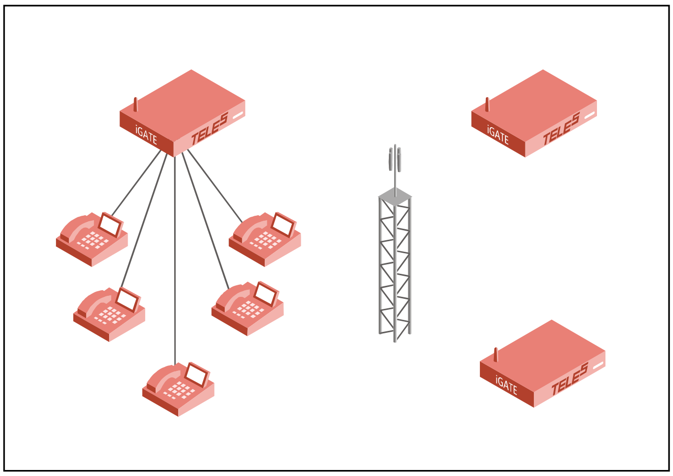
a) **Integration in a carrier network:** One or more mobile gateways are connected to the carrier network. The carrier network routes mobile connections to the individual mobile gateways, which then terminate the mobile calls.



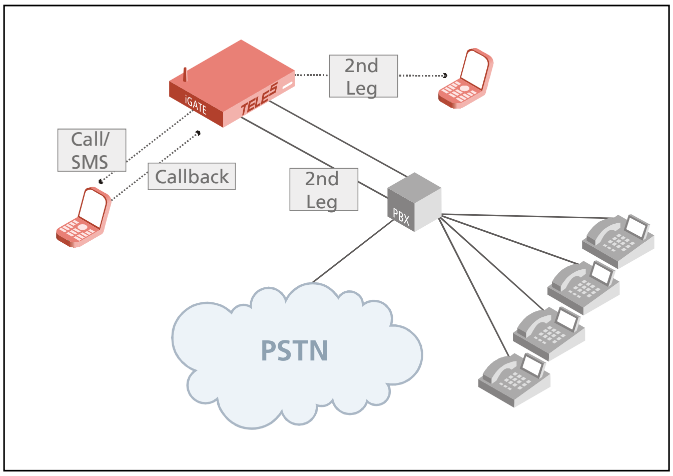
b) **Connection to a centralized SIM server** (vGATE)**:** The mobile gateways are integrated in the vGATE through the IP network. All SIM cards in the vGATE network are installed in and maintained from a central server, so that it is no longer necessary to install SIM cards into each iGATE. The vGateDesktop makes it possible to assign SIMs virtually to random ports and various times without physically removing the SIMs from the vGATE Sim Unit.



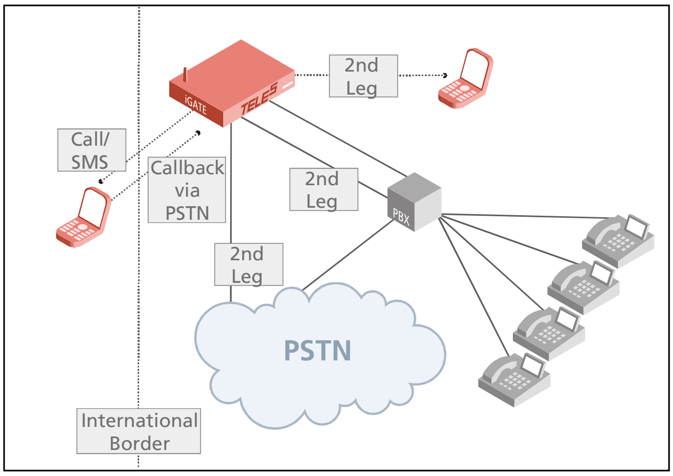
c) **Last mile connection via mobile:** The mobile gateways are set up at specific locations. The mobile gateway can multiplex the available mobile channels, as well as directly connect ISDN subscribers (voice connections only).



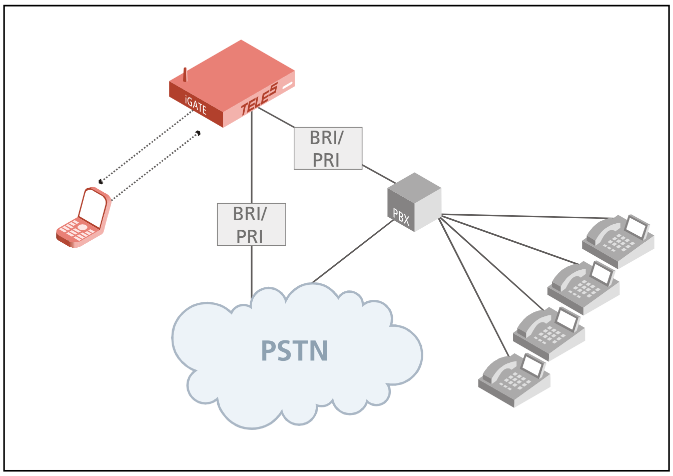
d) **Callback with DTMF:** The user calls a number that is defined so that the user will be called back based on his OAD. An alerting occurs. The user hangs up and is called back. After the user has taken the call, the destination number is entered using DTMF tones. When he has finished dialing, the connection to the destination number is established.



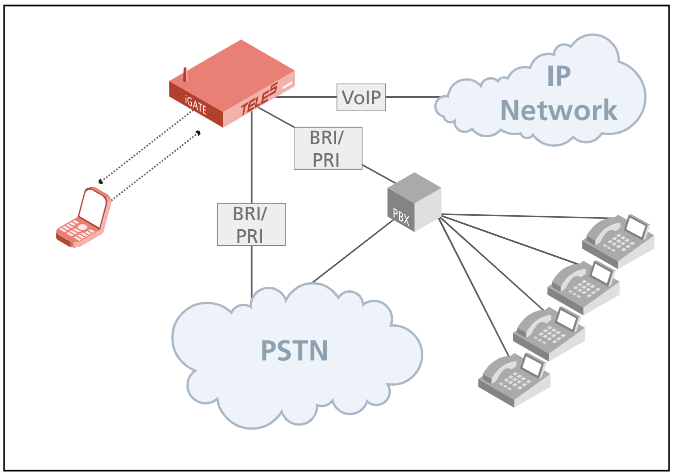
e) **Callback for international roaming:** The user with an international mobile (prepaid SIM) calls a predefined number in the system. An alerting occurs. The user hangs up and is called back based on her OAD. After she accepts the call, she enters the destination number, which is in the same country as the system. This scenario is for employees who travel abroad, as it eliminates high international roaming fees.



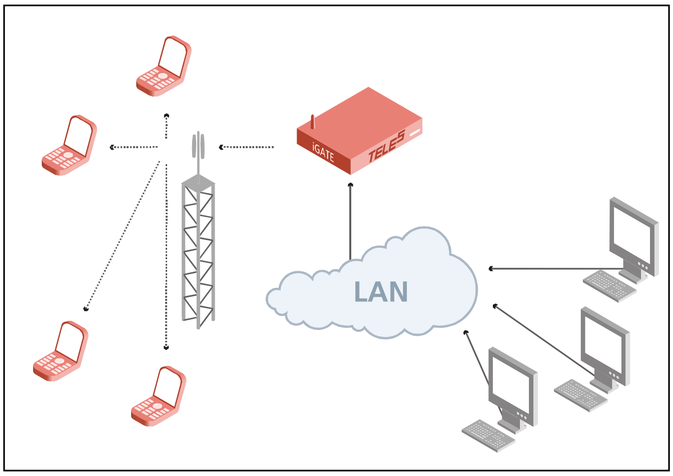
f) **Least Cost Routing for termination of mobile calls:** The mobile gateway with integrated LCR is set up between the existing PBX and the PSTN. The system's LCR recognizes calls to the mobile network and sends them through the mobile gateway to the mobile network.



g) **2nd Generation LCR with VoIP:** One or more mobile gateways are connected to the carrier's IP backbone or the public Internet by VoIP. The carrier network routes mobile connections to the individual mobile gateways, which then terminate the mobile calls accordingly.



h) **Sending SMS by email:** The mobile gateway is connected by Ethernet to the IT network. It implements an SMTP server (e-mail server). Email messages sent to this SMTP server are forwarded to the recipient as SMS messages through the mobile gateway.



4 INSTALLATION

Follow the easy instructions to set up your iGATE in a matter of minutes. Implementation of individual scenarios requires adjustments to the appropriate interfaces. Tips for basic settings are described here. Links to relevant chapters are provided for more specific configuration changes.

4.1 CHECKLIST

The following checklist provides step-by-step installation instructions.

1. Check the package contents
2. Install the device
3. Connect the Ethernet
4. Connect the E1 trunks (optional)
5. Connect the BRI lines (optional)
6. Connect the antennas
7. Using Quickstart, set the configuration (IP address)
8. Check functionality (using the LEDs)
9. Secure the LAN connection
10. Secure connection with the configuration program

4.2 PACKAGE CONTENTS

Your iGATE package contains the following components. Check the contents to make sure everything is complete and undamaged. Immediately report any visible transport damages to customer service. If damage exists, do not attempt operation without customer-service approval:

- 1 iGATE
- 1 power supply cable
- 1 or 2 RJ-45 ISDN cables with gray connectors; 5 meters (optional)
- 1 or 2 RJ-45 ISDN cables with green and blue connectors; 5 meters (optional)
- 1 RJ-45 LAN cable with gray connectors; 3 meters
- 1 copy of quick installation instructions
- 1 CD containing Quickstart, GATE Manager, system manual and default configuration files
- Mobile antennas (optional)

4.3 HARDWARE DESCRIPTION

Throughout this manual, the following boards will be referred to as iGATE 4 Mobile Board, unless otherwise specified:

- iGATE 4 GSM Board
- iGATE 4 CDMA Board
- iGATE 4 UMTS Board

The iGATE is available in expansion levels from 4 to 32 mobile channels. The following pages describe installation of the iGATE.

Figure 4.1 ⇨ shows the rear view of a iGATE, which contains the following boards:

Left side from top to bottom:

- iGATE 4 Mobile Board (for mobile channels 1-4)
- iLCR Base Board
- Optional iGATE Antenna Splitter Board

Right side from top to bottom:

- Optional iGATE 4 Mobile Board (for mobile channels 13-16)
- Optional iGATE 4 Mobile Board (for mobile channels 9-12)
- Optional iGATE 4 Mobile Board (for mobile channels 5-8)

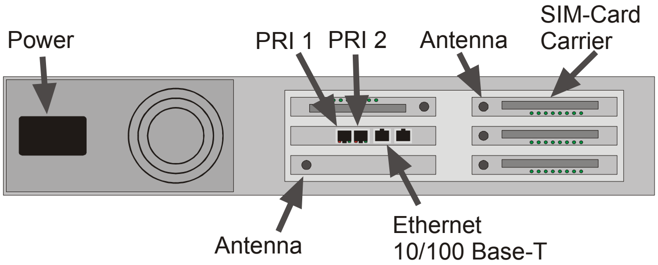


Figure 4.1 2 HU iGATE: Rear View

Figure 4.2 ⇨ shows the rear view of a iGATE BRI, which contains the following boards:

Left side from top to bottom:

- iLCR 4BRI Board
- iLCR Base Board
- One empty slot

Right side from top to bottom:

- One empty slot
- iGATE 4 Mobile Board (for mobile channels 5-8)
- Optional iGATE 4 Mobile Board (for mobile channels 1-4)

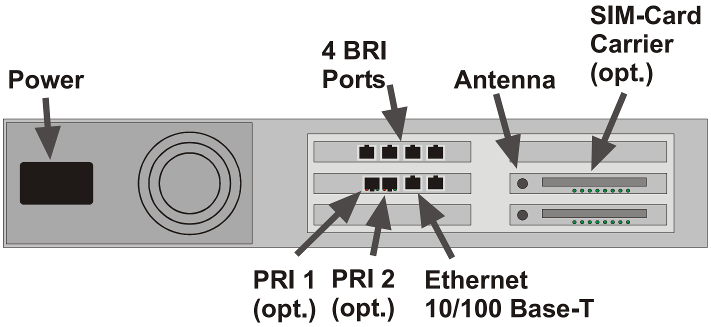


Figure 4.2 2 HU iGATE BRI

Figure 4.3 ⇨ shows the rear view of a TELES.iGATE, which contains the following boards:

From left to right:

- iLCR Base Board
- iGATE 4 Mobile Board (for mobile channels 1-4)
- iGATE 4 Mobile Board (for mobile channels 5-8)
- iGATE 4 Mobile Board (for mobile channels 9-12)
- iGATE 4 Mobile Board (for mobile channels 13-16)
- Optional iGATE Antenna Splitter Board
- iGATE 4 Mobile Board (for mobile channels 17-20)
- Optional iGATE 4 Mobile Board (for mobile channels 21-24)
- Optional iGATE 4 Mobile Board (for mobile channels 25-28)
- Optional iGATE 4 Mobile Board (for mobile channels 29-32)

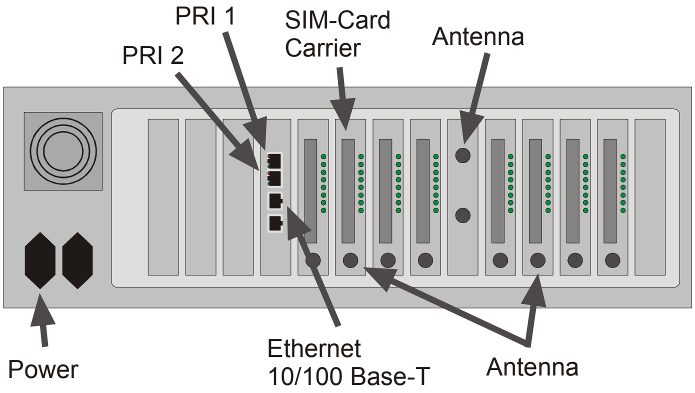


Figure 4.3 4HU iGATE

4.4 INSTALLATION REQUIREMENTS

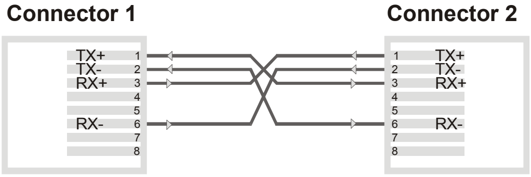
Before installing your iGATE, make sure you have the following connections in place:

- Ethernet connection
- Antenna connection(s)
- Optional ISDN PRI connection to PSTN and/or to the PBX
- Power
- If the system is not connected to a vGATE, insert the SIM cards into the SIM-card carrier, the SIM-card carrier into the iGATE 4 Mobile Board.

4.4.1 ETHERNET WIRING

To connect the iGATE's Ethernet port to your local network, connect the system to an Ethernet switch or hub in your network. Use the three meter cable with gray connectors.

If you want to connect the iGATE directly to your computer and a connection cannot be established, use a cable with the following pin assignment:

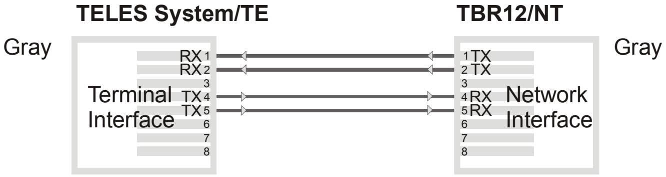


Abbreviations: TX - Transmit / RX - Receive

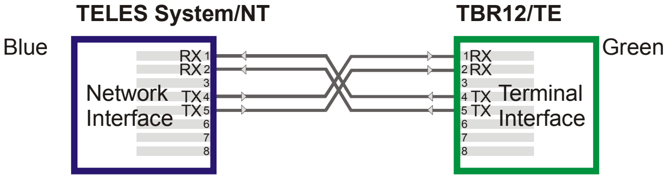
4.4.2 PRI WIRING

4.4.2.1 TELES TO TBR12

If you are connecting a iGATE to E1 and need to change the assignment of an adapter, assign the pins as follows. Connectors on cables included with the iGATE will be gray for TELES TE and gray for NT on the remote device, blue for TELES NT, and green for TE on the remote device:



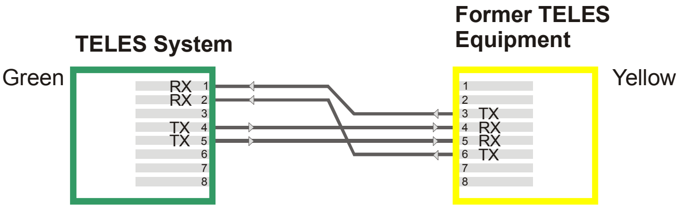
Abbreviations: TX - Transmit / RX - Receive



Abbreviations: TX - Transmit / RX - Receive

4.4.2.2 FORMER TELES ASSIGNMENT TO CURRENT TELES ASSIGNMENT

If you are connecting a system with the former TELES assignment to one with the current TELES assignment, connectors will be yellow for former TE or NT and green for current TE or NT. Pin assignment will be as follows:



Abbreviations: TX - Transmit / RX - Receive

4.4.3 BRI WIRING

If your system contains optional iLCR 4BRI Board, the connection to the PBX or PSTN lines occurs with the RJ45 connectors. Each connector's pin out is for BRI line:

Table 4.1 BRI Wiring

RJ-45	TE	NT	Polarity
3	Transmit	Receive	+
4	Receive	Transmit	+
5	Receive	Transmit	-
6	Transmit	Receive	-

Pins 1, 2, 7, and 8 are not used. TE refers to terminal endpoint (connection to PSTN). NT refers to network termination Layer 1 (connection to PBX).

4.4.4 ANTENNA CONNECTION

Plug an antenna cable into each of the SMA jacks. If the system contains a iGATE Antenna Splitter Board, plug the antenna(s) in there. If not, plug them into the jacks on the iGATE 4 Mobile Board.

Antennas connected to the iGATE must be installed by a qulaified technician according to all necessary safety requirements and the antenna's installation specifications. The antenna adaptor does not provide power surge protection.

4.4.5 SIM CARDS

Each iGATE 4 Mobile Board has a slot for a SIM-card carrier. Insert the SIMs in the SIM-card carrier and then insert the SIM-card carrier into the iGATE 4 Mobile Board.

If the system is connected to a vGATE, the SIM cards will be inserted into the vGATE Sim Unit and not into the iGATE.

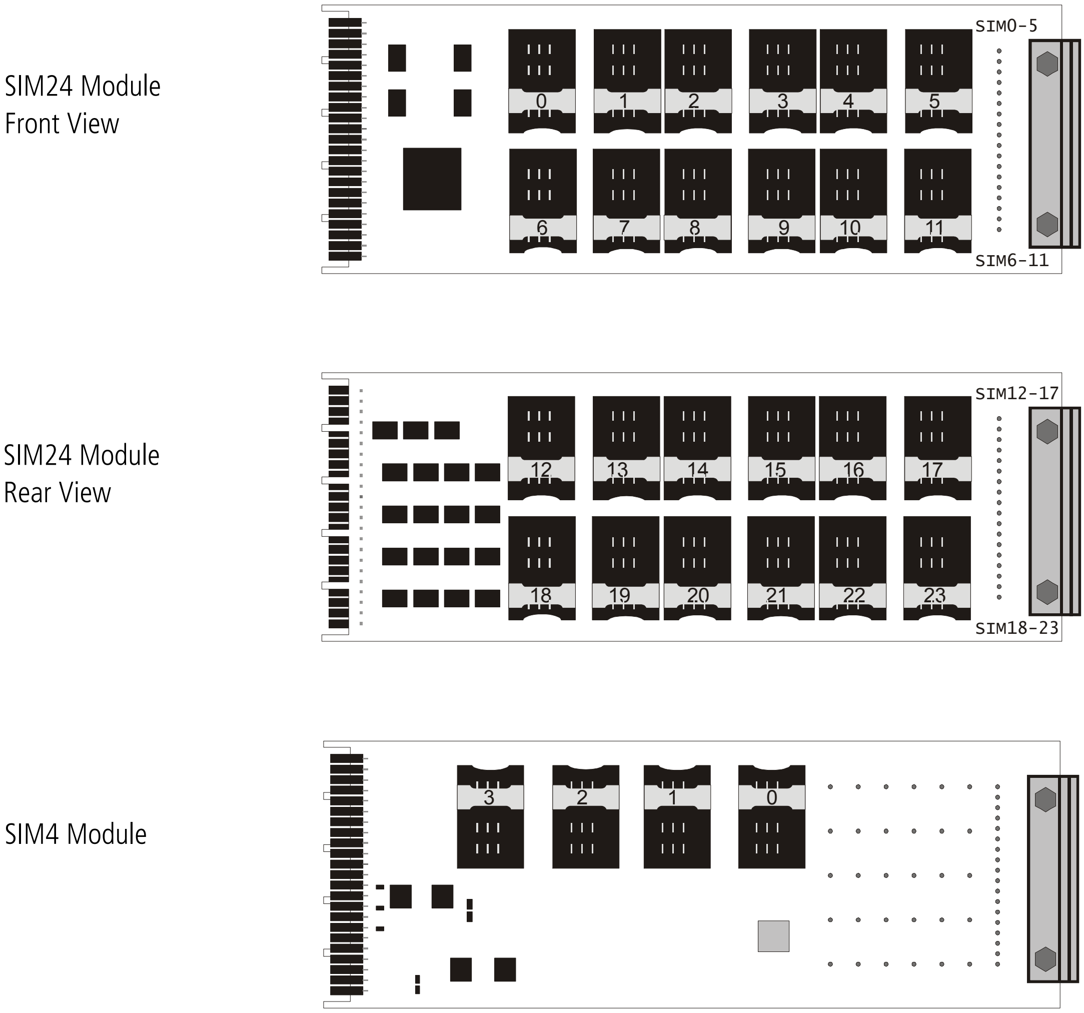
You must configure the PINs in the `pabx.cfg` before inserting the SIM-card carrier unless the SIM has no PIN or the PIN is 0000.

4.4.5.1 THE SIM-CARD CARRIER MODULE

The SIM-card carrier module contains the SIM cards for the individual mobile channels. Each iGATE 4 Mobile Board (standard) contains one module, which can be inserted into and removed from the back of the iGATE 4 Mobile Board during operation. Depending on the modules specifications and version, up to six SIM cards can be implemented in each mobile channel or you can assign SIMs to individual mobile channels as you wish (see `<SIMV>` in Table 5.16 ⇨).

SIM cards are mounted on the front and back of the SIM24 module (optional) or the front of the SIM4 module (Figure 4.4 ⇨). As a guide to help you distinguish top from bottom on the SIM24 module, `SIM0-5` and `SIM12-17` are printed in the upper corner near the module’s blue handle, as shown in Figure 4.4 ⇨. The SIMs on the SIM4 module are numbered from right to left, with one SIM assigned to each mobile channel in ascending order. You can select the SIM cards you would like to use via software. Individual SIM cards on each channel can be active in different Timezones, or they can be reassigned following a time limit or call.

Figure 4.4 SIM-Card Carrier Modules



SIM24 Module Front View

SIM24 Module Rear View

SIM4 Module

Insert ONLY the SIM-card carrier module into the iGATE 4 Mobile Board!

If a SIM24 carrier is used, entries in the subscriber line of the configuration file `pabx.cfg` or in nightfiles refer to the SIM positions for each mobile controller. The SIM positions and mobile controllers correspond with the physical SIM slots on the SIM-card carrier module as shown in Table 4.2 ➪:

Table 4.2 SIM-Card Positions

Slot	Physical Mobile Port per Board	SIM-Card Position
0	1	1
1	2	1
2	3	1
3	4	1
4	1	2
5	2	2
6	3	2
7	4	2
8	1	3
9	2	3
10	3	3
11	4	3
12	1	4
13	2	4
14	3	4
15	4	4
16	1	5
17	2	5
18	3	5
19	4	5

Table 4.2 SIM-Card Positions

Slot	Physical Mobile Port per Board	SIM-Card Position
20	1	6
21	2	6
22	3	6
23	4	6

Example: In the following example, SIMs from various SIM positions in the SIM24 carrier are assigned to individual GSM controllers. Bear in mind that the first GSM controller on the iGATE 4 GSM Board has the physical controller number 00 in the system. SIM 1, which corresponds with slot 0 on the SIM24 carrier, is assigned to the first GSM controller.

Physical Controller Number in the System	Mobile Controller on the iGATE 4 Mobile Board	SIM Card Position for the Mobile Controller	Slot in the SIM24 Carrier
08	1	1	0
09	2	3	9
10	3	2	6
11	4	6	23

```
Subscriber08 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24] CHADDR ALARM NEXT
Subscriber09 = TRANSPARENT ROUTER GSM[0000,00000,+00000,3,1,1,SIM24] CHADDR ALARM
Subscriber10 = TRANSPARENT ROUTER GSM[0000,00000,+00000,2,1,1,SIM24] CHADDR ALARM
Subscriber11 = TRANSPARENT ROUTER GSM[0000,00000,+00000,6,1,1,SIM24] CHADDR ALARM
```

4.5 PREPARING FOR INSTALLATION

Each computer that is to communicate with the iGATE requires a network connection. Please have the following information for connection to your network available:

- IP address in the local network for the iGATE to be configured
- Netmask for the iGATE to be configured
- Default gateway for iGATE to be configured
- DNS server address
- NTP server address

Bear in mind that the preconfigured iGATE's default IP address is 192.168.1.2. If it is already being used in your local network, you must run Quickstart without a connection to your local network. This can occur using a back-to-back Ethernet connection from your computer to the iGATE. If the desired IP address for the iGATE is not in your network, you must assign your computer a temporary IP address from this range.

4.6 HARDWARE CONNECTION

- Connect your computer with the local network
- Connect the iGATE with the local network
- If you choose to connect the iGATE to ISDN, use the ISDN connection cables included in the package contents to connect the iGATE with your PBX and/or the PSTN according to the required port configuration.
- Connect the iGATE to the power supply.

4.7 STARTUP WITH QUICKSTART

Quickstart is an application that helps you to configure the basic settings of your iGATE quickly and conveniently. Quickstart can be installed on any of the following operating systems:

- Windows 98 SE
- Windows NT
- Windows ME
- Windows 2000
- Windows XP
- Windows Vista

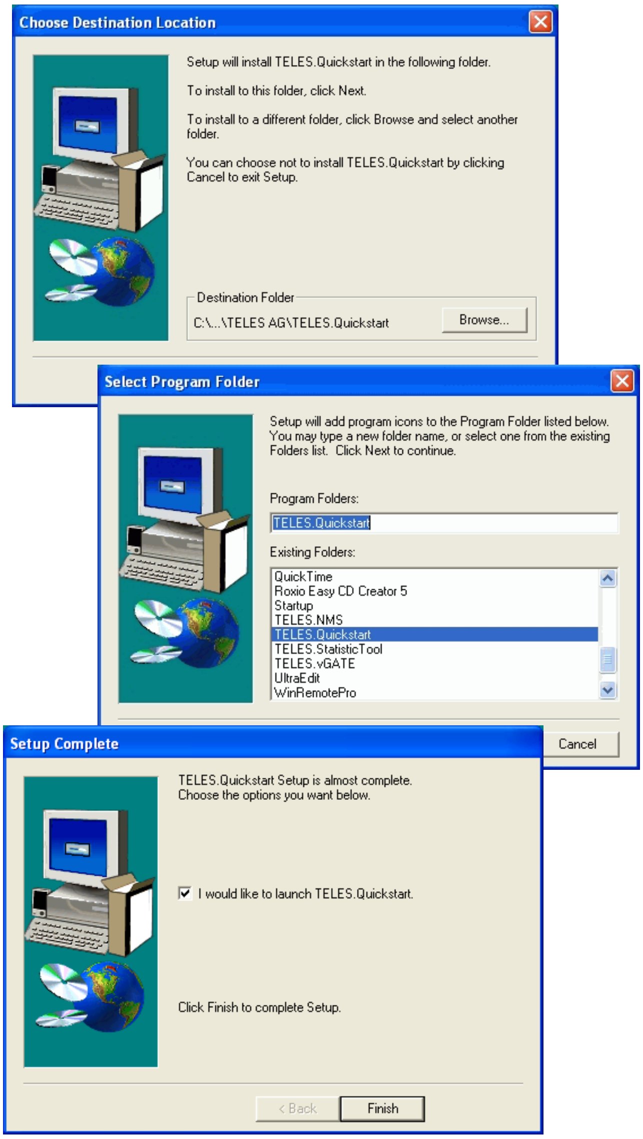
If you are using any of these operating systems, please follow the instructions in this chapter. If you are using a non-Windows operating system (e.g. Linux) follow the instructions in Chapter 4.8 ⇨ .

4.7.1 INSTALLING QUICKSTART

Make sure the GATE Manager is not running on your computer. To install Quickstart on your computer, insert the CD and select Quickstart from the menu. Follow the Windows instructions to begin installation of the Quickstart. Once installation begins, click **Next** to install Quickstart in the predefined folder. To install it in another location, click **Browse** and select a folder from the browser that appears. Then click **Next**.

The next dialog asks you where you want to install the program's icons. To install them in the folder that appears, click **Next**. If you want to install them in another location, select a folder from the list or enter a new folder name. Then click **Next**.

To start Quickstart immediately following installation, activate the checkbox **I would like to launch** Quickstart. Make sure the checkbox is inactive if you do not want to start the program now. Click **Finish**.



Choose Destination Location

Setup will install TELES.Quickstart in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install TELES.Quickstart by clicking Cancel to exit Setup.

Destination Folder: C:\...\TELES AG\TELES.Quickstart

Select Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders: TELES.Quickstart

Existing Folders:

QuickTime
Roxio Easy CD Creator 5
Startup
TELES.NMS
TELES.Quickstart
TELES.StatisticTool
TELES.vGATE
UltraEdit
WinRemotePro

Setup Complete

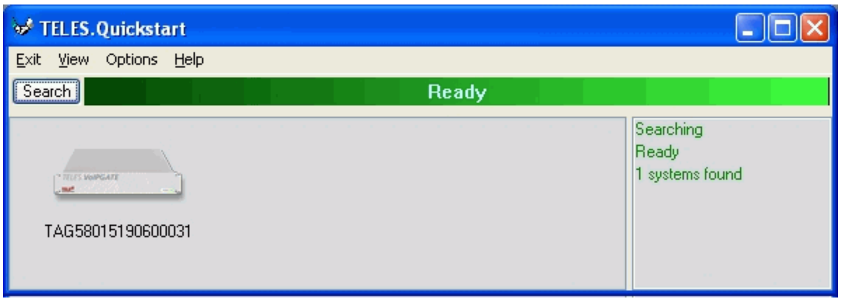
TELES.Quickstart Setup is almost complete. Choose the options you want below.

☑ I would like to launch TELES.Quickstart.

Click Finish to complete Setup.

Figure 4.5 Quickstart Installation

4.7.2 CONFIGURATION WITH QUICKSTART



Searching
Ready
1 systems found

Figure 4.6 Quickstart

Now you can use Quickstart, to set up your iGATE's IP configuration. Open Quickstart`.exe`. The program will automatically search for your iGATE in the local network. For Quickstart, the source UDP port is 57445. It might be necessary to change the firewall rules on your system.

Click the **Search** button if you would like to restart the search. When the program has found your iGATE, it will appear in the window. As soon as it appears, you can end the search by clicking **Stop**.

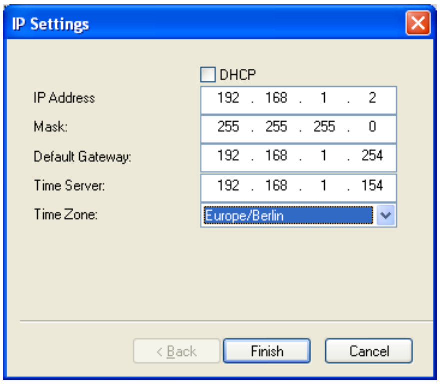
The system's icon will appear in gray if it is unconfigured. Once it has been configured, it will appear in green. The serial number appears as the system's name. The iGATE is partially preconfigured. The configuration files `pabx.cfg` and `route.cfg` are already on the system. Only the system's IP-related entries must be set. Individual port adjustments are to be made manually later. Port properties can be changed and parameters can be assigned then.

To change the appearance of the window, select **Large Icons**, **Small Icons** or **Details** from the **View** menu. In the following description, we will use the Details View, which contains the following columns:

Table 4.3 Quickstart Details View Columns

Heading	Definition
Identifier	This column lists the iGATE's serial number.
IP Address	This column lists the iGATE's IP address.
Configured	An X means the iGATE contains the configuration files.
# of VoIP Ctrls	This column lists the number of VoIP Modules installed in the iGATE. Each VoIP Module represents one VoIP controller.
VoIP Channels	This column shows the number of VoIP channels per VoIP Module.
Type	Lists the type of the system.
Box	An X means the system is a VoIPBOX.
CF Mounted	An X means the iGATE contains a compact flash disk.

To perform the initial configuration of the iGATE, double-click the icon or right-click and select **Configure**. The **IP Settings** dialog will appear. The default IP address appears in the **IP Address** box. Enter a new IP address. If the address you enter already exists in the network, you will be notified to choose another address at the end of the configuration process. Enter the iGATE's netmask in the **Mask** dialog box. Enter the IP address for the **Default Gateway** and the **Time Server** in the corresponding dialog boxes. Select the **Time Zone** for the location of the iGATE. Click **Finish**.



IP Settings

□ DHCP

IP Address: 192 . 168 . 1 . 2

Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 254

Time Server: 192 . 168 . 1 . 154

Time Zone: Europe/Berlin

Figure 4.7 Quickstart Configuration: IP Settings

There is no internal time generation for the system when the power is interrupted. That means the default time is used when the system is restarted or rebooted! Therefore it is important to set the system time with an NTP server.

Now the iGATE is configured; all other processes run automatically.

First the iGATE's IP address will be changed and then the system will start with the new IP address. As soon as the system can be reached at the new IP address, you can set up a GATE Manager connection to the system and check all system information, such as the mobile port status. You can also configure routing entries.

For information on GATE Manager access, see Chapter 4.11 ⇨. For a description of configuration entries, see Chapter 5 ⇨. You will find configuration examples in Chapter 6 ⇨.If you right-click the system's icon in the main window, you can also choose **Temporarily Configure IP Address**, only the IP address for the system's first Ethernet interface address and the netmask will be temporary changed. This can be helpful if you want to set up local remote access to the system and use other IP settings on the remote device than the system's IP configuration in the network. Bear in mind that the functions on the system's first Ethernet interface work with the new settings.

4.8 STARTUP VIA FTP

If you are using a computer that does not use a Windows operating system, you can preconfigure the iGATE via FTP. The iGATE's default IP address is 192.168.1.2. To configure the iGATE using FTP, you must assign your computer an IP address from network range 192.168.1.0 Class C and then access the iGATE via FTP.

The default user is teles and the default password is tcs-ag. To configure the system, use the default configuration file example on the CD in the Configfiles directory and the following four subdirectories:

- `IPconfig`
  This subdirectory contains the file (`ip.cfg`) responsible for configuration of the Ethernet interface.
- `carrier`
  This subdirectory contains a configuration (`pabx.cfg`, `route.cfg`) for iGATE 32 with iGATE 4 GSM Boards and VoIP.
- `corporate`
  This subdirectory contains a configuration (`pabx.cfg`, `route.cfg`) for iGATE 16 with iGATE 4 GSM Boards.
- `umts_system`
  This subdirectory contains a configuration (`pabx.cfg`, `route.cfg`) for iGATE 16 with iGATE 4 UMTS Boards.
- `bri_system`
  This subdirectory contains a configuration (`pabx.cfg`, `route.cfg`) for iGATE 8 with iGATE 4 GSM Boards and an optional iLCR 4BRI Board.

To edit the default configuration, follow the directions in Chapter 5 ➪. Upload the configuration files into the `/boot` directory.

4.9 SELF PROVISIONING WITH NMS

With a management connection to the NMS (Network Management System), the iGATE can retrieve its configuration files from the configured NMS. That means that custom configuration of the device occurs automatically when the device is started. The following setting must be made in the [System] section of the pabx.cfg:

AlarmCallback=<ip address NMS server>

RemoteCallback=<ip address NMS server> <time> <days of week + holiday>

As soon as the device is started, it connects automatically with the NMS, which uses the device's TAG number to send a prepared configuration. For further information on configuration of the NMS, please refer to the NMS Systems Manual.

4.10 LED FUNCTIONALITY

4.10.1 ILCR BASE BOARD PRI PORT LEDS

Each PRI port has one red and one green LED to show the port's status.

The red LED displays the status of the bypass relay that connects the ports with each other when the PRI port's relays are off. That means when the system is connected between a PBX and the PSTN, it is transparent when the LED is red.

The green LED displays whether or not layer 1 is active on the PRI port's connected cable.

Table 4.4 iLCR Base Board PRI Port LEDs

LED	Description
Red on	The system and bypass relay are inactive (normally during the startup phase).
Red off	The system has started and the bypass relay is active.
Green on	Layer 1 is active.
Green off	Layer 1 is inactive.

4.10.2 IGATE 4 MOBILE BOARD SIM-CARD LEDS

On the spine of the iGATE 4 Mobile Board, to the right of the SIM card module, two columns of green LEDs display the status of each mobile channel.

The LEDs in the upper column show the general operational status of the SIM cards, while the status of the mobile channels is displayed in the lower column.

Table 4.5 ⇨ contains a description of the LEDs and what they mean:

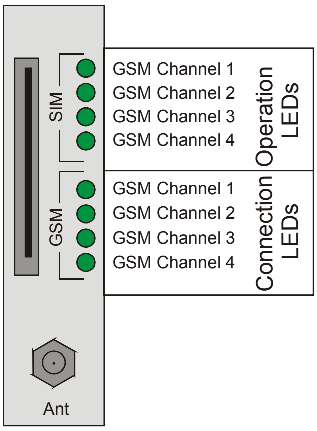


Table 4.5 iGATE 4 Mobile Board LEDs

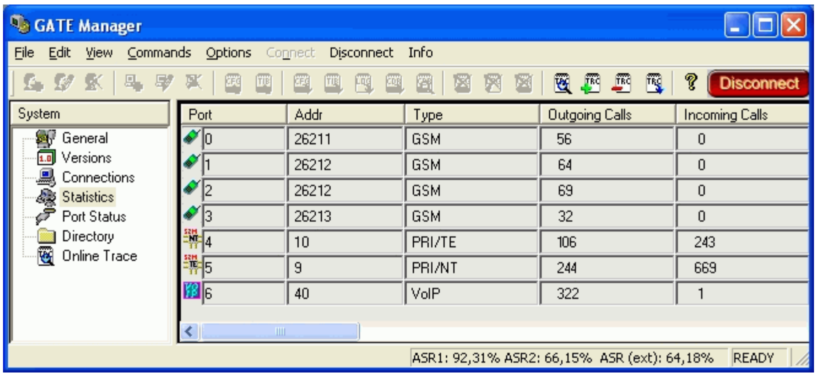
Operational Status	Connection Status	Definition
Off	Off	The mobile channel is not operational because: ▪ No external power supply ▪ SIM module slot is empty ▪ No SIM card
Off	Blinking slowly	Not possible
Off	Blinking quickly	Not possible
Off	On	Not possible

Operational Status	Connection Status	Definition
Blinking slowly	Off	The SIM card is attached, but the mobile channel is not operational because: ▪ Mobile channel is in logon phase ▪ Mobile channel's status is unknown
Blinking slowly	Blinking slowly	Not possible
Blinking slowly	On	Not possible
Blinking quickly	Off	The mobile channel is not operational because: ▪ SIM card has been blocked ▪ Reception field strength below limit
Blinking quickly	Blinking slowly	Not possible
Blinking quickly	Blinking quickly	Status during initializing phase (e.g. system start up). Display changes when status of mobile changes.
Blinking quickly	On	Not possible
On	Off	The mobile channel is operational, the SIM card has logged on.
On	Blinking slowly	Not possible
On	Blinking quickly	The mobile channel is operational, the SIM card has logged on, a connection is being set up on this channel
On	On	The mobile channel is operational, the SIM card has logged on, a connection has been set up on this channel

4.11 REMOTE ACCESS AND ACCESS SECURITY

After the system has been configured and all cables are connected, remote administration and maintenance can occur with the GATE Manager (Chapter 4.11.1 ➪)or via FTP (Chapter 4.11.2 ➪).

4.11.1 GATE MANAGER



Port	Addr	Type	Outgoing Calls	Incoming Calls
0	26211	GSM	56	0
1	26212	GSM	64	0
2	26212	GSM	69	0
3	26213	GSM	32	0
4	10	PRI/TE	106	243
5	9	PRI/NT	244	669
6	40	VoIP	322	1

ASR1: 92,31% ASR2: 66,15% ASR (ext): 64,18% READY

Figure 4.8 GATE Manager

The GATE Manager administration and maintenance software offers a broad range of functions. The GATE Manager is user friendly and can be customized to suit your needs.

The following maintenance functions are possible:

- Display system information and network element status.
- Retrieve and display configuration files.
- Restart network elements.
- Use of a trace option for checking functions and fault diagnosis. Option to use an external tool, e.g. to display and break down trace data.
- Update the system software (firmware) and configuration tables.
- Retrieve CDRs (Call Detail Records).
- Display the current connections (status).
- Display statistical information for network elements and interfaces.
- Display the status of the interfaces.

Use the CD enclosed in your package contents to install the GATE Manager. For a detailed description of installation and implementation of the GATE Manager, please refer to the GATE Manager and Utilities Programs Manual.

GATE Manager remote access can occur via IP or ISDN. GATE Manager access via IP uses port 4444 as origination TCP port and port 4445 as destination port. The following default value (4445) is configured in the `pabx.cfg` file for the system's port:

```
MoipPort=4445
```

In the default configuration, ISDN access is disabled. To configure the system so that certain data calls are received as remote administration calls, make the following changes in the pabx.cfg:

```
RemoteCode=BBB
MapAll<num>=BBB DATA
```

Make the following entries in the route.cfg if the system is to handle all data calls as remote-administration calls:

```
MapAll0=BBB DATA
MapAll1=BBB DATA
MapAll2=BBB DATA
MapAll3=BBB DATA
MapAll4=BBB DATA
MapAll5=BBB DATA
MapAll6=BBB DATA
MapAll7=BBB DATA
MapAll8=BBB DATA
MapAll9=BBB DATA
```

For a detailed description of ISDN configuration, see the TELES Infrastructure Systems Parameters and Hardware Manual.

4.11.2 FTP

Remote access can also occur via FTP. You can use FTP to transfer configuration files. You can also carry out functions and traces with raw commands. Use the username `teles` and the defined password to connect to the system with FTP.

The following entries ensure the security of your FTP access:

Table 4.6 FTP Security Entries

FTP Security
FtpdPort=<port> Defines the FTP access port (default 21).
RemotePassword=<password> Defines the password for FTP and GATE Manager access. Please refer to Chapter 4.11.3 ➩ for instructions on how to enter an encrypted password in the `pabx.cfg`. If you do not define a password, access to the system via GATE Manager occurs without a password, and FTP access occurs with the default password `tcs-ag`.

Once you have access to the system, you will be in the folder `/home/teles`. To upload or download configuration files change to the directory `/boot`. To download log files, change to the directory `/data` if the system contains a flash disk. Otherwise change to the directory `/boot`.

The following commands can be carried out via FTP access:

Table 4.7 FTP Commands

Command	Function
SITE xgboot	Boots the entire system.
SITE xgact	Activates the configuration.
SITE xgact 1-19	Activates the `Night` section corresponding with the number 1-19.
SITE xgtrace 0	Deactivates trace.
SITE xgtrace 1	Activates layer 2 trace.
SITE xgtrace 2	Activates layer 3 trace.

4.11.3 SETTING A PASSWORD FOR REMOTE ACCESS

The following entry ensures the security of your remote access. Use the **mkpwd.exe** tool to generate the password. You will find it on the enclosed CD in the directory `pwd`.

Start the program in a command window with the entry `mkpwd <password>`. The output shows the encrypted password. Enter the encrypted password in the configuration file `pabx.cfg`’s parameter line as follows:

```
RemotePassword=<crypt>
```

When the file has been transferred to the system and the configuration has been activated, access to the system can occur only with the password. Don’t forget to memorize the password!

If you do not define a password, access to the system via GATE Manager occurs without a password, and FTP access occurs with the default password `tcs-ag`.

5 CONFIGURATION FILES

This chapter describes the basic setup and the most commonly used entries for the configuration files. Configuration of iGATEs is managed in the following three files:

Table 5.1 Configuration Files

File	Function
ip.cfg	This file is for the basic configuration of the Ethernet interfaces.
pabx.cfg	This file is for system-specific and port-specific settings.
route.cfg	This file is for routing entries.

Changing configuration data and/or SIM card positions may lead to malfunctions and/or misrouting, as well as possible consequential damage. All changes are made at own risk. TELES is not liable for any possible damage out of or in relation with such changes. Please do therefore thoroughly check any changes you or a third party have made to your configuration.

The system comes without the file ip.cfg. The default configuration with the IP address 192.168.1.2 is active when this file is not on the system. You can configure the system using Quickstart, GATE Manager or via FTP (user teles, password tcs-ag). If you use the HTTP user interface to make configuration changes, the files will be adjusted automatically.

Make sure you secure the system with new passwords following configuration and remember to memorize the passwords!

These configuration files contain all system-specific settings and are used when the system starts. Comments included in these files must begin with a semicolon. They do not need to be at the beginning of a line. Configuration files must end with an empty line.

Please save a backup of the files pabx.cfg and route.cfg before starting configuration.

CONFIGURATION FILES

The configuration files follow these conventions: Individual files are divided into sections. These sections always begin with a line entry in square brackets. The basic required sections are in these files:

Table 5.2 Required Configuration File Sections

Section	File	Function
[System]	pabx.cfg route.cfg ip.cfg	This section contains the system's basic settings.
[Night<num>] EXAMPLE: [Night1] [Night2]	pabx.cfg route.cfg	This section contains time dependent entries that only apply for limited times.
[emac0]	ip.cfg	This section contains the IP configuration for the first Ethernet interface.

5.1 CONFIGURATION FILE IP.CFG

The basic settings for the two Ethernet interfaces are entered here. One interface usually suffices. The second interface can be used for special requirements, e.g. as a hub port, DSL router or vLAN interface. Generally, these settings are entered once and then left unchanged.

This file contains the following sections, which must appear in the order given:

Table 5.3 Sections in the ip.cfg File

Section	Function
[System] (required)	This section contains entries that define the default gateway and/or special routing entries.
[emac0] (required) [emac1] (optional)	The Ethernet Media Access Controller section(s) define the physical Ethernet interface(s).
[nat] (optional)	This section includes settings for Network Address Translation.
[bridge0] (optional)	These section(s) contain settings for the second Ethernet controller in bridge mode.
[pppoe<x>] (optional)	These sections contain settings for direct connection between the system and the DSLAM when the PPPoE protocol is used. `<x>` can be `0` or `1`.
[firewall] (optional)	This section contains settings for activating the system's firewall.

Table 5.3 Sections in the ip.cfg File

Section	Function
[altqd] (optional)	This section enables prioritization of VoIP packets in the iGATE through an IP network using bandwidth control.
[dhcpd] (optional)	This sections contains a list of parameters and settings for the DHCP server in the system. It is divided into global settings for the server and parameters for the DHCP subnet.
[xppp<x>] (optional)	This section contains settings for point-to-point dial-up setup via ISDN.
[vlan<x>] (optional)	These section(s) contain settings for the virtual networks. <x> can be anything from 0 to 9.

5.1.1 SYSTEM SECTION CONFIGURATION

The [System] section contains entries that define the default gateway and/or special routing entries.

To define the standard gateway, use the following entry to set the IP address:

`DefaultGw=<ip addr>`

Example:

```
[System]
DefaultGw=192.168.1.254
```

If you must route specific net ranges to gateways other than what is defined in the default route, make the following entries in the [System] section:

`Route=<target range> -netmask <ip mask> <ip gateway>`

Example:

```
[System]
DefaultGw=192.168.1.254
Route=10.0.0.0 -netmask 255.0.0.0 192.168.1.1
```

If only certain routes apply, leave the line `DefaultGw` empty.

5.1.2 ETHERNET INTERFACE CONFIGURATION

The system includes two Ethernet interfaces (EMAC0 and EMAC1). Only the first is active in the default configuration. Therefore, make sure you plug the cable into the right controller. The second Ethernet interface can be configured as needed.

The following settings are possible for the sections [emac0] (matched to the first Ethernet controller) and [emac1] (matched to the second Ethernet controller):

`IpAddress=<ip addr>/<netmask>`

The IP address is entered in decimal notation, followed by a slash (/) and the netmask in bit notation.

Example:

```
IpAddress=192.168.1.2/24
```

The following entry is used to allocate an IP address via DHCP:

```
IpAddress=dhcp
```

The following entry is used in the `[emac1]` section if operation of the system is occurs in bridge mode.

```
IpAddress=up
```

5.1.3 BRIDGE CONFIGURATION

A bridge can connect two networks with each other. A bridge works like a hub, forwarding traffic from one interface to another. Multicast and broadcast packets are always forwarded to all interfaces that are part of the bridge. This can occur on the Ethernet or VLAN level:

```
BrConfig=add <interface-x> add <interface-y> up
```

Activating another Ethernet interface in this way is useful, for example, when the Ethernet switch does not have any more ports available for connection of the system. You can simply unplug a cable and plug it into the system's second Ethernet interface.

Example:

```
[bridge0]
BrConfig=add emac0 add emac1 up
```

5.1.4 NAT CONFIGURATION

The NAT (Network Address Translation) module translates IP addresses from the local network to an IP address or range on a public interface. All rules are defined in the `[nat]` section:

Table 5.4 NAT Configuration

map=<interface> <local network address/mask> -> <public network address/mask> <optional entries>	
This parameter maps the IP address in the local network to the IP address in the public network.	
<interface>	Defines the translated interface or protocol: emac1 The system's second Ethernet interface pppoe0 Protocol used for DSL connections xppp<0> Protocol used for ISDN and CDMA dial-up connections
<local network address/mask>	The IP address is entered in decimal notation, followed by a slash (/) and the netmask in bit notation. The entire local network range is configured.

Table 5.4 NAT Configuration *(continued)*

<public network address/mask>	Defines the public network range, with network address and mask (usually exactly one address), into which the local IP addresses are to be translated. The IP address is entered in decimal notation, followed by a slash (/) and the netmask in bit notation.
<optional entries>	Special rules can be defined for some services or protocols. The system can serve as a proxy for FTP: proxy port ftp ftp/tcp Special ports for the public address(es) can be assigned for the protocols TCP and UDP. The range is defined by the start and end ports: portmap tcp/udp <start port>:<end port> If no optional entry is defined, all other addresses will be translated without special rules.
rdr=<interface> <public network address/mask> port <port> -> <local network address/mask> port <port_number> <protocol>	
This parameter redirects packets from one port and IP address to another.	
<interface>	Defines the translated interface or protocol: emac1 The system's second Ethernet interface pppoe0 Protocol used for DSL connections Protocol used for ISDN and CDMA dial-up connections
<public network address/mask>	Defines the public network range, with network address and mask (usually exactly one address), into which the local IP addresses are to be translated. The IP address is entered in decimal notation, followed by a slash (/) and the netmask in bit notation.
<port>	Defines the port number.
<local network address/mask>	The IP address is entered in decimal notation, followed by a slash (/) and the netmask in bit notation. The entire local network range is configured.
<protocol>	Defines the protocol. `tcp` and `udp` are possible.

Example: The following NAT settings are for a system in which PPPoE (DSL) is used toward the Internet. The local network range 192.168.1.0 Class C is translated with the following rules:

- The proxy mode is used for FTP.
- All other TCP and UDP packets are mapped to the external ports 40000 to 60000.
- There are no special rules for any other services.
- Incoming requests to port 80 and 443 in the public IP address 192.168.1.100 are redirected to ports 80 and 443 in the local IP address 192.168.1.100.

```
[nat]
map=emac1 192.168.1.0/24 -> 0/32 proxy port ftp ftp/tcp
map=emac1 192.168.1.0/24 -> 0/32 portmap tcp/udp 40000:60000
map=emac1 192.168.1.0/24 -> 0/32
rdr=emac1 0/0 port 80 -> 192.168.1.100 port 80 tcp
rdr=emac1 0/0 port 443 -> 192.168.1.100 port 443 tcp
```

5.1.5 PPPOE CONFIGURATION

The protocol Point-to-Point over Ethernet is used for DSL communication with the DSLAM. That means the system can connect directly with the carrier network and terminate VoIP traffic directly.

All necessary information for setup of the PPPoE connection is defined in the `[pppoe<x>]` section. That means username, password and authentication protocol are set here. The Ethernet interface is emac1 and the gateway can also be defined. The parameter `PppoeIf` defines the physical Ethernet interface used (always emac1). The settings are entered as follows:Bear in mind that configuration of the firewall, the NAT module and prioritization of the VoIP packets must be considered when routing voice and data through the DSL line.

Example: The following entry will create the interface `pppoe0`, with the username `user` and the password `pwd`. The PAP authentication protocol is used. The default route occurs via DSL:

```
[pppoe0]
PppoeIf=emac1
User=user
Pwd=pwd
AuthProto=pap
Route=0.0.0.0
```

5.1.6 FIREWALL SETTINGS

The firewall settings provide options for limiting or denying access to and from the system. If you do not configure this section, the firewall is inactive and access is unlimited.

Make sure you configure the firewall rules carefully. The rules are processed from top to bottom. If you use the option `quick`, you will break the sequence. We recomend that you put the most restrictive rule at the end of the configuration.

Example: In the following example, only port 4445 allows incoming connections from the IP address 192.168.1.10. All others will be blocked.

```
[firewall]
fw=pass in quick on emac0 proto tcp from 192.168.1.10/32 to any port
eq 4445 flags S keepstate keep frags
fw=block in log quick on emac0 all
```

Table 5.5 Settings in the `[firewall]` Section of the `ip.cfg`

[firewall] **fw=<mode> <direction> <list>**	
<mode>	Two modes are possible for permitting or denying access: pass permits access block denies access
<direction>	Possible directions are in and out: in external to internal out internal to external
<list>	All other entries specify the other settings for the corresponding firewall rules and are optional. The order in the line is as listed below:
log Records non-matching packets.	
quick Allows short-cut rules in order to speed up the filter or override later rules. If a packet matches a filter rule that is marked as quick, this rule will be the last rule checked, allowing a short-circuit path to avoid processing later rules for this packet. If this option is missing, the rule is taken to be a "fall-through rule, meaning that the result of the match (block/pass) is saved and that processing will continue to see if there are any more matches.	
on <interface> The firewall rule is used only for the defined interface (e.g. emac0, pppoe0).	
from <networkaddress/mask> to <networkaddress/mask> from defines the source IP-address range for incoming packets. to defines the target IP-address range for outgoing packets. The IP address appears in decimal notation, followed by a slash (/) and the netmask in bit notation. any stands for all IP addresses (e.g.: to any). **NOTE: If you use the rule pass in/out in combination with the option from <ip> to <ip>, you must specify a protocol number with proto and a port number. If you not specify the port, the system may not be reachable.** EXAMPLE: fw=pass in quick on pppoe0 proto tcp from any to any port eq 4445	
proto <protocol> defines the protocol, for which the rule is valid (e.g.: proto tcp, proto udp, proto icmp).	

Table 5.5 Settings in the `[firewall]` Section of the `ip.cfg` *(continued)*

[firewall] **fw=<mode> <direction> <list>**
port eq <num> <num> defines the port as number (e.g.: port eq 4445).
keep state Ensures that the firewall checks packets from the beginning to the end of a session. This is necessary, as the firewall does not know when a session begins or ends.
flags S Only syn. packets are accepted and recorded in the state table. In conjunction with keep state, packets from sessions that have been inactive will also be routed. The advantage of this entry is that random packets will not be accepted.
keep frags Fragmented packets are also routed.

Example:

```
[firewall]
; loopback
fw=pass in quick on emac0 all
fw=pass out quick on emac0 all

; traffic to outgoing
fw=pass out quick on pppoe0 proto tcp all flags S keep state keep frags
fw=pass out quick on pppoe0 proto udp all keep state keep frags
fw=pass out quick on pppoe0 proto icmp all keep state keep frags

; incoming traffic
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 21 flags S keep state keep frags
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 23 flags S keep state keep frags
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 4445 keep state

; icmp traffic
fw=pass in quick on pppoe0 proto icmp all keep state

; other will be blocked
fw=block in log quick on pppoe0 all
fw=block out log quick on pppoe0 all
```

5.1.7 BANDWIDTH CONTROL

In many implementation scenarios, the iGATE in router mode (e.g. as DSL router) sends voice and data traffic through a connection with limited bandwidth. This can lead to lost voice packets that arrive too late to be used in the voice stream. To avoid lost packets, this QOS setting prioritizes packet transmission. You must set the priority for voice signaling and for the voice packets. That means you must prioritize SIP/H.323, RTP and RTCP. You will find the ports used in Table 5.13 ⇨, in the following entries:

`H225Port`

`SipPort`

`VoipRtp Port`

VoipRtpPortSpacing

Different ports can be used for RTP and RTCP, depending on the configuration.

The parameter VoipRtpPort shows the first RTP port used. The corresponding RTCP port is the next one up. The parameter VoipRtpPortSpacing shows the next RTP port (RTP port + port spacing).

Table 5.6 Settings in the [altqd] Section of the ip.cfg

interface <interface> bandwidth <bw> priq	
Defines the interface for which the rule applies.	
<interface>	Sets the interface for which prioritization apples (e.e. pppoe0).
<bw>	Sets the bandwidth that is available on the interface in Kbit/s (e.g. 256K).
priq	Priority qeueing. A higher priority class is always served first.
class priq <interface> <class> root priority <prio>	
Defines the priority of the filter entries.	
<class>	Two types can be set: ▪ realtime_class (VoIP packets) ▪ regular_class (data packets)
<prio>	Enter a value between 0 and 15. The higher the value (e.g. 15), the higher the priority.
filter <interface> <class> <values>	
Defines the individual rules for the class.	
<values>	The individual values are divided into the following entries. A 0 can be entered as a wildcard, in which case all values are possible: ▪ <dest_addr> (can be followed by netmask <mask>) ▪ <dest_port> ▪ <src_addr> (can be followed by netmask <mask>) ▪ <src_port> ▪ <protocol tos value>: 6 for TCP 17 for UDP

Example: In the following example, prioritization is set for a thirty-channel VoIP connection. The SIP signaling port 5060 and the RTP/RTCP ports 29000 to 29059 are prioritized at level 7. All other services are set at level 0:

```
[altqd]
interface pppoe0 bandwidth 512K priq
class priq pppoe0 realtime_class root priority 7
  filter pppoe0 realtime_class 0 5060 0 0 0
  filter pppoe0 realtime_class 0 0 0 5060 0
  filter pppoe0 realtime_class 0 29000 0 0 17
  filter pppoe0 realtime_class 0 0 0 29000 17
  filter pppoe0 realtime_class 0 29001 0 0 17
  filter pppoe0 realtime_class 0 0 0 29001 17
  ....
  filter pppoe0 realtime_class 0 29058 0 0 17
  filter pppoe0 realtime_class 0 0 0 29058 17
  filter pppoe0 realtime_class 0 29059 0 0 17
  filter pppoe0 realtime_class 0 0 0 29059 17
class priq pppoe0 regular_class root priority 0 default
```

5.1.8 DHCP SERVER SETTINGS

The DHCP (Dynamic Host Configuration Protocol) server provides a mechanism for allocation of IP addresses to client hosts. The section `[dhcpd]` contains a list of parameters and settings for the DHCP server in the system. It is divided into global settings for the server and parameters for the DHCP subnet.

Table 5.7 Settings in the [dhcpd] Section of the ip.cfg

; Global dhcp parameters
allow unknown-clients; All DHCP queries are accepted and the configured settings are transmitted to the clients.
ddns-update-style none; Deactivates dynamic update of the domain name system as per RFC 2136.
; Parameters for the Subnet

subnet <network address> netmask <mask for network range> {
<list>
}

In <list> you can enter any of the following specific network settings activated by the DHCP server. Each oprion must begin in a new line and end with a semicolon (`;`).
range <start IP address> <end IP address>; The DHCP network range is defined by the first and last address in the range. Client assignment begins with the last address.
option broadcast-address <IP address>; Defines the broadcast address for the clients in the subnet..
option domain-name "<string>"; Defines the domain name used in the network.

Table 5.7 Settings in the [dhcpd] Section of the ip.cfg *(continued)*

; Global dhcp parameters
option domain-name-servers <IP address>; Defines the DNS-server address to be assigned (as per RFC 1035) All of the following optional entries defining server addresses are also transmitted as per RFC 1035. Separate multiple addresses per server with a comma: `… <IP address>, <IP address>;` (this also applies for all other optional entries with IP addresses).
option netbios-name-servers <IP address> Defines the WINS-server address to be assigned.
option ntp-servers <ip address>; Defines the NTP-server address to be assigned.
option time-servers <ip address>; Defines the time-server address to be assigned (RFC 868).
option routers <IP address>; Defines the router address to be assigned.
option subnet-mask <net mask>; Defines the netmask to be assigned (as per RFC 950).

option tftp-server-name "<link>";
Defines the TFTP server name (option 66), as per RFC 2132.
EXAMPLE: option tftp-server-name "http://192.168.0.9";

Example:

```
[dhcpd]
; Global dhcp parameters
allow unknown-clients;
ddns-update-style none;

; Parameter for the Subnet
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.3 192.168.1.20;
 option broadcast-address 192.168.1.255;
 option domain-name "company.de";
 option domain-name-servers 192.168.1.100;
 option routers 192.168.1.2;
 option subnet-mask 255.255.255.0;
}
```

5.1.9 PPP CONFIGURATION FOR ISDN AND CDMA DIAL-UP

The point-to-point protocol is used for dial-up connection via ISDN lines or via a mobile CDMA connection. That means the system can set up an Internet connection, which can be used for all local users or to transmit VoIP calls via ISDN dial-up. Make sure you configure the firewall and NAT options accordingly.

The advantages of VoIP over ISDN can be seen especially in corporate implementation. For example, it is useful when a very high number of connections occurs between subsidiaries and one subsidiary does not have a broadband Internet connection. An ISDN B-channel can be connected to the Internet and up to six voice calls can occur simultaniously over one ISDN line. All necessary information for setup of the PPP connection is defined in the section `[xppp<num>]`.

The settings are entered as follows:

Table 5.8 Settings in the `[xppp]` Section of the `ip.cfg`

[xppp<num>]
Dad=<num> Enter the dial-up number. Only digits can be defined here. Any required special characters (* or #) can be set in the mapping entry.
User=<username> Enter a username.
Pwd=<password> Enter a password.
Route=<ip-addr> Enter the target IP address range, e.g. 0.0.0.0 (default route).
AuthProto=<protocol> Enter `chap` or `pap` for the protocol used for authentication.
IdleTO=<sec> Enter the number of seconds without traffic before the interface tears down the connection.
MTU=<int> Maximum Transfer Unit. We recommend the following default values: 1500 for ISDN dial-up and 120 for CDMA dial-up.
Rfc1662=<val> Framing to be used: 0 for ISDN or 1 for CDMA
LcpTO=<msec> Allows you to change the value of the LCP timeout. The timeout-value must be specified in milliseconds (default 1000).
StartDelay=<sec> Time in seconds the system will wait to start the ppp process.

Example:

```
[xppp0]
Dad=12345
User=user
Pwd=pwd
Route=0.0.0.0
AuthProto=chap
IdleTO=60
MTU=1500
Rfc1662=0
LcpTO=500
StartDelay=10
```

5.1.10 VLAN CONFIGURATION

A VLAN (Virtual Local Area Network) is a virtual LAN within a physical network. Each VLAN is assigned a unique number (VLAN ID) and defined in the `[vlan<x>]` section with

Tag: value between 1 and 4095

Priority: value between 0 and 7 (0 is lowest and 7 is the highest priority)

```
[vlan0]
IfConfig=vlan <tag>,<priority> vlanif <interface>
```

Example: The following entry will create the interface vlan1, with VLAN tag 10 and priority 7, on the Ethernet interface emac0. Following this configuration, IP addresses (and/or other protocols) can be assigned to the vlan1 interface:

```
[vlan1]
IfConfig=vlan 10,7 vlanif emac0
IpAddress=192.168.199.1
```

5.1.11 EXAMPLES

5.1.11.1 DEFAULT CONFIGURATION

In the following example, the system's IP address is 192.168.1.1, the netmask is 255.255.255.0, and the standard gateway is 192.168.1.254:

```
[System]
DefaultGw=192.168.1.254

[emac0]
IpAddress=192.168.1.1/24
```

5.1.11.2 ACTIVE ETHERNET BRIDGE

In the following example a two-port Ethernet bridge is configured. The system's IP address is 192.168.1.1, the netmask is 255.255.255.0, and the standard gateway is 192.168.1.254, The emac1 interface is active and both Ethernet interfaces are set to bridge mode in the `[bridge0]` section:

```
[System]
DefaultGw=192.168.1.254

[emac0]
IpAddress=192.168.1.1/24

[emac1]
IpAddress=up

[bridge0]
BrConfig=add emac0 add emac1 up
```

5.1.11.3 INTEGRATED DSL-ROUTER SCENARIO FOR VOIP TRAFFIC WITH AN ACTIVE DHCP SERVER AND FIREWALL

In the following example, the system is connected to the local IP network through emac0. The DSL modem is connected to the emac1 interface, which enables the system to connect directly to the carrier network without an additional router when the connection is used only for VoIP data. A DHCP server is used for dynamic IP-address allocation:

```
[System]

[emac0]
IpAddress=192.168.0.2/24

[emac1]
IpAddress=up

[pppoe0]
PppoeIf=emac1
User=usertelekom
Pwd=pwd
AuthProto=chap
Route=default

[nat]
map=pppoe0 192.168.0.0/24 -> 0/32 proxy port ftp ftp/tcp
map=pppoe0 192.168.0.0/24 -> 0/32 portmap tcp/udp 40000:60000
map=pppoe0 192.168.0.0/24 -> 0/32

[firewall]
; loopback
fw=pass in quick on emac0 all
fw=pass out quick on emac0 all

; traffic to outgoing
fw=pass out quick on pppoe0 proto tcp all flags S keep state keep frags
fw=pass out quick on pppoe0 proto udp all keep state keep frags
fw=pass out quick on pppoe0 proto icmp all keep state keep frags

; incoming traffic
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 21 flags S keep state keep frags
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 23 flags S keep state keep frags
fw=pass in quick on pppoe0 proto tcp from 10.4.0.0/16 to any port eq 4445 keep state

; icmp traffic
fw=pass in quick on pppoe0 proto icmp all keep state

; other will be blocked
fw=block in log quick on pppoe0 all
fw=block out log quick on pppoe0 all

[dhcpd]
; Global dhcp parameters
allow unknown-clients;
ddns-update-style none;
; Parameter for the Subnet
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.3 192.168.1.20;
 option broadcast-address 192.168.1.255;
 option domain-name "company.de";
 option domain-name-servers 192.168.1.100;
 option routers 192.168.1.2;
 option subnet-mask 255.255.255.0;
```

5.1.11.4 VLAN SCENARIO

In the following example, the system is connected to the IP backbone through emac0. One Computer is connected to the emac1 interface. You can separate voice and data traffic with two different VLANs (vlan0 with tag 10 for voice, vlan1 with tag 11 for data). All traffic coming from emac1 will be sent to vlan1. Voice and data will not be mixed:

```
[System]
[emac0]
IpAddress=192.168.1.12/16

[emac1]
IpAddress=up

[vlan0]
IfConfig=vlan 10,7 vlanif emac0
IpAddress=10.0.1.2/24

[vlan1]
IfConfig=vlan 11,1 vlanif emac0
IpAddress=172.16.4.5/16

[bridge0]
BrConfig=add vlan1 add emac1 up
```

5.2 CONFIGURATION FILE PABX.CFG

The `pabx.cfg` file contains system-specific settings and the port configuration. It is divided into the [System] and [Night<num>] sections.

5.2.1 SYSTEM SETTINGS

The [System] section is divided into several categories to ensure clarity.

- Life line (relay)
- Log files
- Night configuration
- Controllers
- Subscribers
- Global settings
- SMTP-client configuration
- Number portability settings

The following subchapters contain a detailed description of these categories.

5.2.1.1 LIFE LINE

The entry in this category is responsible for the life-line (bypass) functionality of the PRI port’s relay when the system is on. When the system is off, both PRI ports are connected to each other, which means that it provides a transparent connection between the PBX and the PSTN. When the system is on, all routing algorithms are active.

```
Bypass=ON/OFF
```

`ON`: PRI relay is on (system controls both PRI ports).

`OFF`: PRI relay is off (both PRI ports are connected to each other, regardless of whether or not the system is running).

This parameter should always be set to ON.

5.2.1.2 LOG FILES

CDRs, unconnected calls, system events, trace output and statistics can be saved into files.

The following entries are necessary to generate log files:

Table 5.9 pabx.cfg: Log File Entries

Entry	Description
ActionLog=/data/protocol.log	System events
Log=/data/cdr.log	CDR entries
RRufLog=/data/failed.log	Unconnected calls
TraceLog=/data/trace.log	System trace
MsgLog=/data/msg.log	Incoming SMS and USSD messages

The path in the example refers to an optional external flash disk. If there is no external flash disk, the path will be: `boot`.

Example:

```
ActionLog=/boot/protocol.log
```

The available internal memory is approximately 8 MB if the iGATE does not contain optional memory expansion. Make sure you monitor the available memory.

You can define how the log files are to be divided. There are two possibilities for saving entries into a new file:

- In increments of time (twice-daily, daily, weekly, monthly)
- Depending on the size of the file

You can also define a maximum number of up to 35 files to be generated.

A dash (-) appears in place of information that is to be ignored.

Table 5.10 pabx.cfg: Log Parameters

Log=/data/<file.log> <saved> <size> <number>	
<file>	The name of the log file is generated as follows: [file]yymmdd[0-9|A-Z].log.
<saved>	Refers to the frequency with which the file is saved. The following options are possible: halfdaily Every day at 11:59 and 23:59 daily Every day at 23:59 weekly Sunday at 23:59 monthly The last day of the month at 23:59
<size>	Regardless of the value entered in <saved>, the file will be saved when the <file size> has been reached. **NOTE: We recommend a file size of a multiple of 60kB.**
<number>	Refers to the number of files that will be saved in the system (between 5 and 35) before the first file is overwritten. This setting is useful not only for limited file size, but also for files that store events. Normally size can be limited for these files, e.g. 5 files of 1MB each. If the fifth file is full, the first one will automatically be overwritten.

Example 1 In the following entry, the files `cdr.log` and `failed.log` are renamed every day or when the file reaches 180kB, whichever comes first. Up to 7 CDR files will be saved on the system. If the file size reaches 180kB on one day, the second file will have the same date. Only the running number will be increased.

```
Log=/data/cdr.log daily 180 7
RrufLog=/data/failed.log daily 180 7
```

Example 2 In the following entry, the file protocol.log is renamed every day or when the file reaches 60 kB. Up to 21 failed files will be saved on the system.

```
ActionLog=/data/protocol.log daily 60 21
```

Example 3 In the following entry, the file `trace.log` is renamed every day when the file has reached 600kB. Up to seven log files will be saved on the system.

```
TraceLog=/data/trace.log daily 600 7
```

Example 4 In the following entry, the statistic values are reset daily at 12:00 midnight and saved in the `asr.log`.

```
StatisticTime=/data/asr.log 00:00 11111111
```

Please remember to keep track of how much memory is available on the system.

5.2.1.3 NIGHT CONFIGURATION

The sections for the time-dependent configuration changes and time-controlled routings are defined here.

A maximum of 19 additional daily configuration zones are possible (`Night1` to `Night19`). The entry NightResetTime reactivates the original configuration contained in the System section.

The entry will have the following syntax:

Table 5.11 pabx.cfg: Night Parameters

Night<num>=<time> <day>	
<num>	Enter a value between 1 and 19 to define which configuration is to be loaded.
<time>	If there is a time set with the format `hh:mm` after this entry, this configuration is loaded at that time on the defined day.
<day>	Use a bitmask to set the weekdays on which the configuration applies here. The daymap appears in the following order: HoSaFrThWeTuMoSu.

Example:

The configuration section is activated Fridays, Wednesdays and Mondays at noon unless the day in question is a holiday:

```
Night2=12:00 00101010
```

The configuration section switches back to the default configuration (`System` section) every day at 8:00 p.m:
NightResetTime=20:00 11111111

Any defined `Night` sections must be set in the files `pabx.cfg` and `route.cfg`. If there are no changes in these sections, you must copy them from the System section. The complete Subscriber section must appear in the Night section of the pabx.cfg (see Chapter 5.2.5 on page 75 ⇨). The active route(s) (MapAll, Restrict and Redirect entries) must appear in the Night section of the route.cfg (see Chapter 5.3 on page 76 ⇨).

5.2.1.4 CONTROLLERS

This category defines the parameters that apply to the ports. The order of the ports is defined as follows: The iGATE contains integrated iGATE 4 Mobile Boards, each of which contain four mobile modules. Each iGATE 4 Mobile Board's mobile channels are configured as additional controllers. That means four controllers are configured for each board. Beginning with 0, these controllers are defined as the first controllers in the section. Next the PRI controllers are defined, followed by the VoIP controllers. All controllers are defined in ascending order.

Table 5.12 ➪ describes the order for additional boards.

Table 5.12 Configuration Order: Controller Parameters

Function	Number of Controllers
iLCR 4BRI Boards	Up to 4 (optional)
iGATE 4 Mobile Boards	Up to 32 (optional)
iLCR Base Board (PRI)	2
iLCR Base Board (VoIP)	Up to 4 (optional)
DTMF (virtual)	Up to 1 (optional)

Table 5.12 ➪ shows only the maximum number of controllers for each individual interface. Any possible combinations will depend on the system's specifications!

The individual ports are defined with the following parameter:

Table 5.13 pabx.cfg: Controller Parameters

Controller<port>=<bus> <type> <mode> <line_type> ADR:<address> IRQ:<interrupt> UNIT: VALUE:	
<port>	Defines the running (physical) port number.
<bus>	Defines the configured (virtual) port number. In the default configuration, PRI TE ports are 9 and PRI NT ports are 10. VoIP ports are 40.
<type>	Defines the connection type: TES2M PRI external (terminal endpoint) NTS2M PRI internal (network termination) VOIP VoIP module GSM GSM port CDMA CDMA port UMTS UMTS port TE BRI external (if you change from NT to TE or vice versa, you must change the DIP switches for the respective port on the iLCR 4BRI Board) NT BRI internal DTMF virtual controller for activating DTMF tone recognition
<mode>	Defines the protocol variation for PRI and BRI lines: DSS1 SS7 (only for PRI lines) CAS R2(only for PRI lines)

<line_type>	Switches CRC4 mode for PRI lines on or off:
	CRC4 CRC4 on
	DF double frame: CRC4 off
	Additional entry for SS7 only:
	FIS Increases the volume FISU messages. To avoid a high volume of D-channel traffic on these controllers, use this keyword only if necessary.
	Additional entry for T1 only:
	T1 US Defines this controller as T1. Bear in mind that if one controller is defined as T1, all controllers must be thus defined. If you configure T1, you must also enter CHMAX[23] in the corresponding Subscriber lines.
	T1 EXAMPLE:
	`Controller00=20 TES2M DSS1 T1 US`
	`Controller01=21 NTS2M DSS1 T1 US`
	`...`
	`Subscriber00 = TRANSPARENT ROUTER CHMAX[23]`
	`Subscriber01 = TRANSPARENT ROUTER CHMAX[23]`

Table 5.13 pabx.cfg: Controller Parameters *(continued)*

Controller<port>=<bus> <type> <mode> <line_type> ADR:<address> IRQ:<interrupt> UNIT: VALUE:	
<address>	(Optional) Defines the hardware address used for the first controller on an additional iGATE 4 Mobile Board. These entries are preconfigured and cannot be changed.
<interrupt>	(Optional) Defines the interrupt used for the first controller on an additional iGATE 4 Mobile Board. These entries are preconfigured and cannot be changed.

UNIT:	(Optional) Defines the currency for the charges (default EUR). Special charge generation is possible. Special charge generation is possible for:
	France UNIT:&F
	Spain UNIT:&SP
	Portugal UNIT:&P
	Greece UNIT:&G
	Switzerland
	UNIT:&CH
	Netherlands
	UNIT:&NL
	Italy UNIT:&I
	NOTE: The <line_type> must be configured for these entries to work.
	EXAMPLE:
	`Controller02=10 NT DSS1 PMP UNIT:€ VALUE:0.010`
	`Controller03=10 NT DSS1 PMP UNIT:€ VALUE:0.010`

VALUE:	(Optional) Defines the charges that accumulate by unit (default 12).

Ports set to the same type can have the same bus number. In this case they will form a trunk group. If you change this parameter in the configuration, you must restart the system.

Example 1 Each iGATE 4 Mobile Board contains 4 controllers. The hardware address and the interrupt are defined behind the first controllers, which are defined in the configuration before the iLCR Base Board. In the following example, the system contains four iGATE 4 Mobile Boards. One PRI controller is configured for TE and one for NT. The protocol used is DSS1, and CRC4 is active. One VoIP Module is attached.

```
Controller00=20 GSM ADR:D800 IRQ:5
Controller01=20 GSM
Controller02=20 GSM
Controller03=20 GSM
Controller04=20 GSM ADR:D900 IRQ:7
Controller05=20 GSM
Controller06=20 GSM
Controller07=20 GSM
Controller08=20 GSM ADR:DA00 IRQ:5
Controller09=20 GSM
Controller10=20 GSM
Controller11=20 GSM
Controller12=20 GSM ADR:DB00 IRQ:7
Controller13=20 GSM
Controller14=20 GSM
Controller15=20 GSM
Controller16=9 TES2M DSS1 CRC4
Controller17=10 NTS2M DSS1 CRC4
Controller18=40 VoIP
```

Example 2 Each iGATE 4 CDMA Board contains 4 controllers. The hardware address and the interrupt are defined behind the first controllers. These are defined in the configuration before the optional iLCR 4BRI Board. The hardware address and the interrupt for this board is also defined behind its first controller. The last controllers are for the iLCR Base Board. In the following example, the system contains 2 iGATE 4 CDMA Boards, a iLCR 4BRI Board with 4 controllers. One PRI controller is configured for TE and one for NT. The protocol used is DSS1, and CRC4 is active.

```
Controller00=30 NT DSS1 PMP ADR:C000 IRQ:11
Controller01=30 NT DSS1 PMP
Controller02=30 NT DSS1 PMP
Controller03=30 NT DSS1 PMP
Controller04=20 CDMA ADR:D800 IRQ:5
Controller05=20 CDMA
Controller06=20 CDMA
Controller07=20 CDMA
Controller08=20 CDMA ADR:D900 IRQ:7
Controller09=20 CDMA
Controller10=20 CDMA
Controller11=20 CDMA
Controller12=9 TES2M DSS1 CRC4
Controller13=10 NTS2M DSS1 CRC4
```

Example 3 Each iGATE 4 UMTS Board contains 4 controllers. The hardware address and the interrupt are defined behind the first controllers, which are defined in the configuration before the iLCR Base Board controllers. In the following example, the system contains 2 iGATE 4 UMTS Boards. One PRI controller is configured for TE and one for NT. The protocol used is DSS1, and CRC4 is active. One VoIP Module is attached.

```
Controller00=20 UMTS ADR:D800 IRQ:5
Controller01=20 UMTS
Controller02=20 UMTS
Controller03=20 UMTS
Controller04=20 UMTS ADR:D900 IRQ:7
Controller05=20 UMTS
Controller06=20 UMTS
Controller07=20 UMTS
Controller08=9 TES2M DSS1 CRC4
Controller09=10 NTS2M DSS1 CRC4
Controller10=40 VoIP
```

5.2.1.5 SUBSCRIBERS

Various functions for individual interfaces (ISDN or VOIP) are defined in each controller's `Subscriber` line. The order of the subscriber lines is the same as the order of the controller lines (see Chapter 5.2.1.4 on page 60 ➪). Most changes become active following a restart. If it suffices to activate the configuration, this is noted in the parameter description: Additional parameters for mobile controllers are described in Table 5.15 ➪ and Table 5.16 ➪. The parameters listed in Table 5.15 ➪ are required for mobile controllers and those listed in Table 5.16 ➪ are optional, depending on the implementation scenario.

Table 5.14 pabx.cfg: Subscriber Parameters

Subscriber<port>=<list>	
<port>	Defines the running (physical) port number.
The <list> variable may contain one or more of the following keywords:	
DEFAULT	The standard configuration will be used. No other parameters in this table are set.
TRANSPARENT ROUTER	Only the number is sent as caller ID (without the virtual port address). Activate configuration suffices to activate changes.
CASR2[<name>]	Activates the profile defined in the corresponding [CASR2] section.
ALARM	Activates the monitoring mode for the respective port. If a relevant error occurs at the port, a remote call is placed to the number defined in `RemoteCallBack`. Activate configuration suffices to activate changes.
SWITCH	Changes internal port handling. In the default configuration, the VoIP controller is set to NT. You can use this parameter to change it from NT to TE. Restart the system to activate the changes.
CHMAX[xx]	Defines the number of channels per VoIP controller (VoIP Module), e.g. 16 or for the virtual DTMF controller. This figure must be entered in double digits. A maximum of six concurrent channels are possible for DTMF recognition. **NOTE: If all six channels are used, no PPP dialup or remote access via ISDN is possible.**
DTMF[<sec>,/<dir>/<file>]	Please refer to Chapter 11.2.1.1 ➪.

Required Mobile Parameters

Specific settings for each mobile interface appear in square brackets behind the keywords **GSM**, **UMTS** or **CDMA**. These parameters are separated with a comma.

The following parameters are required:

Table 5.15 Required Parameters in `pabx.cfg`

Subscriber<port>=<type>[<pin>,<lain>,<SMSC>,<sim>,<loudGSM>,<loudPCM>,SIM<x>,...]	
<port>	Defines the running (physical) port number.
<type>	Defines whether a GSM, CDMA or UMTS module is used.
<pin>	Defines the SIM card's PIN. The PIN is always four digits. If no PIN is defined for a SIM card, the PIN 0000 must be used. **NOTE: An error message appears in the protocol.log file when a PIN is incorrectly configured.**
<lain>	Defines the LAIN (**L**ocal **A**rea **I**dentification **N**umber) – the mobile network to be used. This prevents roaming into another mobile network. The LAIN is always five digits. If the LAIN is set at 00000, roaming will not be prevented. The LAIN configuration prevents accidental logon of the SIM card with another network and the use of false SIM cards.
<SMSC>	Defines the SMS center's access number. The number must always begin with + and the country code.
<SIM>	Defines the SIM card to be used. You can enter the values 1, 2, 3, 4, 5, 6 (optional when using the 24 SIM card carrier). Default 1. Do not change the default entry if you use the parameter `SIM4` or `SIMS`. Activate configuration suffices to activate changes. **NOTE: Please see the example following Table 5.16 ⇨ for information on numbering SIM cards.**
<loudGSM>	Defines the volume level for the mobile line. The values 0 to 3 are possible. 0 is loudest and 3 is the least loud.
<loudPCM>	Defines the volume level to the fixed network. The values 0 to 7 are possible. 7 is loudest and 0 is the least loud.
SIM4	Defines the SIM-card carrier used. The number entered (4) refers to the number of slots. The SIM-cards can be distributed among the 4 mobile channels at will. **NOTE: This parameter cannot be used in combination with SIM24, SIMS and SIMV.**
SIM24	Defines the SIM-card carrier used. The number entered (24) refers to the number of slots. The SIM-cards can be distributed among the 4 mobile channels at will. **NOTE: This parameter cannot be used in combination with SIM4, SIMS and SIMV.**

Optional Mobile Parameters

In addition to the usual parameters, you can enter the following optional mobile parameters. Separate each parameter with a comma.

Table 5.16 Optional Parameters in `pabx.cfg`

Optional Mobile Parameters
<IMSI> This keyword causes the IMSIs to be recorded in each CDR. This parameter appears after `SIM<x>`. Activate configuration suffices to activate changes.
SIMS Define this keyword to connect the system to a vGATE. `SIM1` must be defined in the appropriate mobile controller `Subscriber` line. **NOTE: This parameter cannot be used with the following parameters: `SIM24`, `SIM4` and `SIMV`. Bear in mind that no SIM-card carrier is to be inserted in the iGATE.** EXAMPLE: Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIMS]
SIMV Define this keyword to assign a SIM to a mobile controller. The specific SIM (1-24) must also be defined. **NOTE: This parameter cannot be used with the following parameters: `SIM24,` `SIM4` and `SIMS`.** EXAMPLE: Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,12,1,1,SIMV]

Table 5.16 Optional Parameters in `pabx.cfg` *(continued)*

Optional Mobile Parameters
BAND(<int>) **For iGATE 4 UMTS Boards:** Defines the mobile standard used and `(<int>)` can have the following values: `0` = autonegotiation (default) `1` = UMTS `3` = GSM **For GSM Q24CL001 modules:** Defines the GSM frequency band and (<int>) can have the following values: `1` = Mono-band mode 850MHz `2` = Mono-band mode 900MHz `3` = Mono-band mode 1800MHz `4` = Mono-band mode 1900MHz `5` = Dual-band mode 850/1900MHz `6` = Dual-band mode 900/1800MHz `7` = Dual-band mode 900/1900MHz After changing the band settings, you must restart the system to activate the changes. **NOTE: The BAND parameter can only be used with quad-band GSM module-type Q24CL001. These quad-band GSM modules are available as of hardware revision 1.61 (May, 2007). There is no default band setting! If there is no BAND configuration in the pabx.cfg when the system is started, the last band stored on the module will be used. This can cause the system to attempt to register the SIM with the wrong GSM band.**

Example: The following example has two groups of SIMs. Different SMS center numbers are set for controllers 00-07 and 08-15. SIM 24 Carriers are used, so that several SIMs can be used for each mobile channel. SIM-position 1 is used in the SIM 24 Carrier for the first, third and fourth iGATE 4 Mobile Board (SIM-slots 0-3). SIM-position 2 is used in the second iGATE 4 Mobile Board SIM-slots 4-7). Routing to mobile is based on the LAIN (**CHADDR**):

```
Subscriber00 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIM4,IMSI] CHADDR ALARM NEXT
Subscriber01 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber02 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber03 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIM4,IMSI] CHADDR ALARM

Subscriber04 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,2,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber05 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,2,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber06 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,2,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber07 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,2,1,1,SIM4,IMSI] CHADDR ALARM

Subscriber08 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM NEXT
Subscriber09 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber10 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber11 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM

Subscriber12 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber13 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber14 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM
Subscriber15 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIM4,IMSI] CHADDR ALARM

Subscriber16 = TRANSPARENT ROUTER ALARM
Subscriber17 = TRANSPARENT ROUTER ALARM
Subscriber18 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
```

For a detailed description of the configuration of the iGATE 4 Mobile Board, including the keywords `CHADDR`, `NEXT`, `LIMIT` and `CONTINUE`, please refer to Chapter 7 on page 95 ⇨.

5.2.1.6 GLOBAL SETTINGS

This category contains the following system parameters:

Table 5.17 pabx.cfg: IP Configuration System Parameters

System Parameters
VoipGlobalMaxChan=<count> Max. number of channels for the entire system.
VoipRtpPort=<port> Defines the starting UDP port used to transmit RTP packets (default 29000).
VoipRtpPortSpacing=<count> Defines the space between the ports used for individual RTP streams (default 2).
H225Port=<port> Endpoint-to-endpoint port (default 1720).
SipPort=<port> Sip signaling port (default 5060).

Table 5.17 pabx.cfg: IP Configuration System Parameters *(continued)*

System Parameters
VoipMaximumBandwidth=<int> Defines an upper limit for available bandwidth for the VoIP profiles to be configured (see VoipBandwidthRestriction in Table 9.6 ⇨) if traffic shaping is active for the corresponding VoIP profile. Individual codecs are assigned the following values: g711a, f711u, trp: 8 g72632, t38: 4 g72624 3 g72616, gsm 2 Other 1 You must define the list of codecs to be used in the VoIP profiles, whereby the codec with the highest priority must be defined first. Calls will be set up using the codec with the highest priority as long as the sum of the values for individual calls remains lower than defined here. If the sum is greater, the next call will be set up with, and existing calls will be switched to, a higher compression rate. Bear in mind that the VoIP peer must support this feature.
VoipStrictRfc3261=<mode> If yes is set, the SIP transaction/dialog matching will occur strictly as per RFC3261. You must disable this feature for peers that use RFC2543 (from and to name). Default is yes.
StunServerAddress=<ip addr> When this parameter is active, the iGATE looks for a (NAT) firewall in the network and figures out how to bypass it without requiring changes. All ports for signaling, RTP and RTCP are checked. The parameter VoipGlobalMaxChan defines the number of ports for RTP and RTCP. **NOTE: This is not a solution for all firewall types.**
StunServerPollInterval=<sec> Interval (in seconds) for the stun request at each port (default 600).
Radius=<mode> On (default) activates the Radius service. If you change Off to On, you must restart the system.
RadiusAuthPort=<num> Port used for Radius authentication (default 1812).
RadiusAcctPort=<num> Port used for Radius accounting (default 1813).
NameServer=<ip addr> IP-address configuration for the DNS server. Enter your network or ISP’s DNS server. If you don’t know it, you can also enter another DNS server. If you have more than one address, enter this parameter up to three times on different lines.

Table 5.17 pabx.cfg: IP Configuration System Parameters *(continued)*

System Parameters
Timezone=<continent/city> Defines the time difference between the iGATE's time zone and time zone 0 (Greenwich Mean Time). Enter the continent and a large city (usually the capital) in the time zone.

NtpServer=<ip addr>
Sets the IP address at which the iGATE's SNTP server queries the standard time. The query occurs every four hours.
NOTE: If your system is not attached to an NTP server, you can enter the following configuration to query the time on an attached PBX via a TE port:
Subscriber=...TIME

Clockmaster=<type> Enter S0 to take the system clock from the BRI port if the system has an additional BRI board and special firmware installed on which at least one controller is connected to the PSTN in TE mode. This parameter only makes sense if the system does not have a PRI port connected to the PSTN.
S2MLongHaul=<mode> This option increases the sensitivity on PRI receiving side to support Long Haul applications. The default value is **No** (Short Haul).
MoipPort=<port> Defines the GATE Manager access port (default 4445).
FtpdPort=<port> Defines the FTP access port (default 21).
TelnetdPort=<port> Defines the TELNET access port (default 23).
TftpdPort=<port> Defines the TFTP access port (default 69).
Ftpd=<mode> Activates (on) or deactivates (off) FTP access. Default on.
Telnetd=<mode> Activates (on) or deactivates (off) TELNET access. Default on.
Tftpd=<mode> Activates (on) or deactivates (off) FTP access. Default off.

Table 5.17 pabx.cfg: IP Configuration System Parameters *(continued)*

System Parameters
RemotePassword=<password> Defines the password for FTP and GATE Manager access. Please refer to Chapter 4.11.3 ⇨ for instructions on how to enter an encrypted password in the pabx.cfg. If you do not define a password, access to the system via GATE Manager occurs without a password, and FTP access occurs with the default password tcs-ag.
SimCtrlUnitAddress=<ip addr> Enter the vGATE Control Unit's IP address. For a detailed description of iGATE configuration for connection to a vGATE, see Chapter 7.1 ⇨.
DialTone=<country> If the system is used in a corporate settings and attached through a PBX to the PSTN, it may be necessary to generate the carrier's dial tone. It depends on whether the system sends the dialed digits to the PSTN or whether it waits for a routing entry to take the call. The following values can be entered: GE DE IR UK US FR IT

Example:

```
VoipGlobalMaxChan=60
H225Port=1720
SipPort=5060
VoipRtpPort=29000
VoipRtpPortSpacing=2
NameServer=192.168.0.254
Timezone=Europe/Berlin
NtpServer=192.168.0.254
DialTone=GE
```

There is no internal time generation for the system when the power is interrupted. That means the default time is used when the system is restarted or rebooted! Therefore it is important to set the system time with an NTP server. If the system is connected via BRI or PRI, a clock may come from the network connected to the corresponding port. Enter `!TIME` in the `pabx.cfg`'s `subscriber` line and then activate the configuration to block this clock.

5.2.2 SMTP-CLIENT CONFIGURATION

The following entries in the pabx.cfg's [Mail] section are used to send e-mail messages from the iGATE. The connection to the SMTP server can be used to send CDR files, incoming SMS to an e-mail account or alarm messages.

You must restart the system after making changes to activate the settings.

The following features are possible:

- Sending SMS via e-mail
- Receiving SMS in an e-mail, SMS or in a file
- Sending and receiving USSD text messages
- Displaying incoming calls via e-mail
- Setting up connections using e-mail
- Sending announcements via e-mail
- Sending automatic SMS for unconnected calls
- Sending CDRs via e-mail
- Sending alarm messages via e-mail

SmtpServer=<ip addr>

In <ip addr>, enter the IP address of the destination SMTP server that is to receive the e-mail messages.

MailUserIn=<username>

Enter a username for incoming e-mail authentication.

MailUserOut=<username>

Enter a username for outgoing e-mail authentication.

MailPwdIn=<password>

Enter a password for incoming e-mail authentication.

MailPwdOut=<password>

Enter a password for outgoing e-mail authentication.

MailAuthEncr=<type>

Enter an encryption method for e-mail authentication (default base64).

MailRcpt=<domain>

In <domain>, enter the destination domain, the destination address and an @ sign. If the destination address is already complete (with an @ sign), <domain> is not added.

MailFrom=<domain>

In <domain>, enter the source domain, the source address and an @ sign. If the source address is already complete (with an @ sign), <domain> is not added.

MailRcvMax=<count> Maximum number of incoming e-mails queued for transmission via SMS or USSD.
MailRcptMax=<count> Number of "RCPT TO" entries in e-mails that come from the LAN (a message is sent to the LCR for each "RCPT TO" entry in each incoming e-mail).
MaxMailsToHost=<count> Maximum number of e-mail messages sent to the LCR simultaneously.
MailToHostDelay=<count> Number of seconds until an e-mail message is sent to the LCR (this timer runs separately for each MaxMailsToHost message).
MailToHostRetries=<count> Number of retries when SMS transmission is not successful. When the limit entered is reached, an error message is sent to the e-mail sender (default 3).
MailSendRetries=<count> Number of times an attempt is made to send an e-mail.
MailMaxIncomingClients=<count> Defines the maximum number of clients that can access the system simultaneously. If 0 is entered, the SMTP port (25) will be blocked for incoming sessions. Default 5.
MailTcpRcvTimeout=<sec> Defines the number of seconds after which a session will be terminated following a possible receiving error in the data stream. Default 0 (immediately).
MailTcpSndTimeout=<sec> Defines the number of seconds after which a session will be terminated following a possible transmission error in the data stream. Default 0 (immediately).
MailAllowedPeers=<ip addr> Defines IP addresses from which incoming SMTP connections will be accepted. Separate IP addresses with a space. If a dash (-) is entered, the SMTP port (25) will be blocked for incoming sessions. If this parameter is left empty (default), incoming connections will be accepted from all IP addresses.
MailPropPort=<num> Enter the port number for a TELES proprietary mail protocol.

Example:

```
[Mail]
SmtpServer=172.16.0.10
MailRcpt=teles.de
MailFrom=172.16.0.100
MailRcvMax=500
MailRcptMax=100
MaxMailsToHost=2
MailToHostDelay=3000
MailToHostRetries=10
MailSendRetries=10
MailAllowedPeers=172.16.0.10
```

Sending Alarm Messages via E-mail

With the appropriate configuration, you can send e-mails containing alarm messages that are written into the log file. The sender is given as `alarm` and the system’s name appears in the subject box. The text box contains the alarm message.

The following entry in the configuration file activates this function:

```
...
ActionLog=/data/protocol.log daily 1000 5 @<e-mail account>
...
```

5.2.3 NUMBER PORTABILITY SETTINGS

The [NumberPortability] section includes the parameters necessary for communication with the database server. For a description of the functionality and configuration of this feature, please see Chapter 11.6 ⇨.

You must restart the system after making changes to activate the settings.

MNPQAddress=<ip addr>

Enter the IP address to which the number portability query is to be sent. The service comes from an external provider. It is also used as the iMNP address if the parameter MNPQSum=Yes is set.

MNPQPort=<port>

Enter the port to which the number portability query is to be sent.

MNPQAddress2=<ip addr>

Enter the IP address to which the second number portability query is to be sent when ! appears in the mapping entry. A second database will then be queried, for example if the first on is not online.

MNPQPort2=<port>

Enter the port to which the second number portability query is to be sent.

MNPQSum=<mode>

This parameter must be activated (Yes) if a iMNP is used.

E2EMRSAddress=<ip addr>

Enter the IP address to which the number portability query is to be sent. The service comes from an external provider.

E2EMRSPort=<port>

Enter the port to which the number portability query is to be sent.

Example:

```
[NumberPortability]
MNPQAddress=172.16.0.100
MNPQPort=9003
MNPQSum=Yes
```

5.2.4 SNMP SETTINGS

The Simple Network Management Protocol facilitates network management and monitoring of iGATE network devices and their functions. For a detailed description of SNMP configuration, please refer to Chapter 12.2 ⇨.

You must restart the system after making changes to activate the settings.

5.2.5 TIME-CONTROLLED CONFIGURATION SETTINGS

The [Night<num>] section is reserved for prospective time-controlled configuration changes. In the `pabx.cfg` file, the `Night` sections contain all of the system's `Subscriber` entries.

Individual SIM-card positions can be configured here. For a detailed description of time-controlled SIM switching, please refer to Chapter 7.10 ⇨

5.2.6 .CAS R2 SETTINGS

If you are working with Channel Associated Signaling, you must activate a CAS profile in the relevant `Controller` and `Subscriber` entries and define the profile in a separate `[CASR2:<name>]` section.

Generally you will need to set only the country code 55 for Brazil. The default country code is 0, which sets the ITU-T standard.

Example:

```
Controller00=9 TES2M CASR2
...
Subscriber00 = TRANSPARENT ROUTER CASR2[BRAZIL] ALARM
...
[CASR2:BRAZIL]
CountryCode=55
```

You must restart the system after making changes to activate the settings.

5.3 CONFIGURATION FILE ROUTE.CFG

The system's routing information is saved in the `route.cfg`. The file contains the following sections:

- [System]
  Contains all routing entries (MapAll, Restrict, Redirect) that are to be active when the default configuration is used.
- [Night<num>]
  Contains all routing entries (MapAll, Restrict, Redirect), and VoIP, gatekeeper and registrar profiles that are to be active with the defined time configuration. Bear in mind that you must also copy all routing and profile settings that may already appear in the das System section or in the individual profile sections, even if they do not change!
- [VoIP:<name>]
  Contains all settings necessary for communication with the VoIP peer.
- [GateKeeper:<name>]
  Contains all settings for the gatekeeper. This profile is then assigned to the VoIP profiles.
- [Registrar:<name>]
  Contains all settings to register with the registrar.

5.3.1 ENTRIES IN THE [SYSTEM] SECTION

The[System]section contains the following entries.

5.3.1.1 MAPPING

Mapping entries begin with the keyword MapAll.

Table 5.18 route.cfg: Map Parameters

MapAll<direct>=<num> <mode>	
<direct>	Defines the prefix or telephone number for which the entry applies.
<num>	Defines the following in the order given: ▪ Destination port's controller number ▪ Optional VoIP profile name followed by a colon if the call is terminated via VoIP ▪ Optional prefix ▪ Part of the number on the left that is to appear on the right The special symbol ? may be used as a wildcard to represent any digit.
<mode>	VOICE Applies for calls with the service indicator **voice** (default). DATA Applies for calls with the service indicator **data**.

Example: In the following example, all mobile calls with the prefix 01555 are transmitted to the mobile controllers (20). All international calls are sent to the VoIP carrier (40) with the profile name DF. All national calls are sent to the PRI controller with the number 9:

```
MapAll01555=|2001555<<14
MapAll00=40DF:00
MapAll0=90
```

If CHADDR appears in the mobile port's Subscriber lines, the entry will look like this:

MapAll<num>=<lain><num>

Example: In the following example, all calls with the prefixes 01555 and 01556 are sent to the mobile controllers with the LAIN 26212. All calls with the prefixes 01444 and 01445 are sent to the mobile controllers with the LAIN 26213. Digit collection is activated:

```
MapAll01555=|2621201555<<17
MapAll01556=|2621201556<<17
MapAll01444=|2621301444<<17
MapAll01445=|2621301445<<17
```

Make sure that the numbers for the carriers are routed to the correct ports! For detailed information on digit collection and enblock/overlap receiving, see Chapter 8.1 ⇨.

5.3.1.2 RESTRICT

This entry is for controller-specific routing entries. These entries apply only for a single controller and can be set for an OAD base number or an MSN:

Table 5.19 route.cfg: Restrict Parameters

Restrict<ns>=<pl> <sin>	
<ns>	Defines the virtual controller number plus an optional base number or a specific calling number.
<pl>	Stands for a virtual placeholder used for the mapping entry that routes calls for the the Restrict command.
<sin>	The service indicator variable sin restricts the command to a service. Without a sin, the Restrict command is valid for all services. Possible service indicator values are: 00 All services 01 Telephony 02 Analog services 03 X.21-services 04 Telefax group 4 05 64 kbps videotext or TELES-specific SMS services 06 TELES-specific USSD services 07 Data transfer 64 kbps 08 X.25-services 09 Teletext 64 10 Mixed mode 15 Videotext (new standard) 16 Video telephone
<time>	Optional. For type 2 redirect entries, a timer (in seconds) can be defined after the service indicator entry. **NOTE: In the entry is to apply for all service indicators, the value 00 must be defined for <sin>.**

Example: In the following example, all calls from PRI controller `9` (PSTN) are sent to PRI controller `10` (PBX) without regard to the routing file:

```
Restrict9=pl
MapAllpl=10
```

Example: In the following example, calls from mobile controllers with the LAIN 26212 are sent to PRI controller 10 (PBX), extension 0. This is imperative, since the caller cannot dial an extension directly with mobile:

```
Restrict26212=100
```

For a detailed description, see Chapter 7.4 ⇨.

5.3.1.3 REDIRECT

This entry facilitates alternative routing when the first destination cannot be reached or is busy. A placeholder appears to the right of the equal sign. The routing entry (MapAll) can be defined for the redirect using the placeholder entered:

This function requires the LCR license.

Table 5.20 route.cfg: Redirect Parameters

Redirect<type><num>=<redirect> <sin> <time>	
<type>	Enter 2, 3 or 5 to set the following types: 2 call forwarding no answer 3 call forwarding when busy 5 call forwarding when busy and no answer
<num>	Defines the number for which calls will be redirected.
<redirect>	Defines the placeholder used in the two-target routing entry and the number to which calls to <x> will be redirected.
<sin>	The service indicator variable sin restricts the command to a service. Without a sin, the Restrict command is valid for all services. Possible service indicator values are: 01 Telephony 02 Analog services 03 X.21-services 04 Telefax group 4 05 Videotext (64 kbps) 07 Data transfer 64 kbps 08 X.25-services 09 Teletext 64 10 Mixed mode 15 Videotext (new standard) 16 Video telephone **NOTE: Fax forwarding must be set for analog and telephony services because incoming fax calls from the analog network may arrive with either telephony or analog service indicators.**
<time>	Enter a number of seconds between 1 and 60. For type 2 only.

Example: In the following example all mobile calls with the prefix 01555 are transmitted to the mobile carrier with the LAIN 26212. Digit collection is activated. If the carrier cannot be reached or is busy, the redirect command activates the second target mapping with the placeholder A and the call is automatically sent to PRI controller 9.

```
MapAll01555=|2621201555<<17
Redirect326212=A
MapAllA=9
```

Excluding Busy Calls or Specific Cause Values from Redirect

Defines a hexadecimal cause value according to DSS1. When connections to the destination are rejected because of the reason defined by the cause value, the iGATE sends a busy signal to the attached PBX. Alternative routing is not carried out.

To avoid second-choice routings when the called-party number is busy, set the following parameter in the first-choice port's Subscriber line in the pabx.cfg:

BUSY[<cause>]	Defines a hexadecimal cause value according to DSS1. When connections to the destination are rejected because of the reason defined by the cause value, the iGATE sends a busy signal to the attached PBX. Alternative routing is not carried out. You can also define a range of consecutive cause values: BUSY[<cause>,<cause>]

Example: In the following example, all outgoing calls over controller 04 are rejected with the cause value 91 when the called party is busy. Alternative routing is not carried out.

```
Subscriber04=....BUSY[91]
```

5.3.1.4 SETTING THE TIME-CONTROLLED SECTIONS

If you use a time-configured route on the system, please see Chapter 5.2.1.3 ⇨ for a definition of individual configuration zones. The active route is configured in the route.cfg file.

The following example contains three sections ([System], [Night1] and [Night2]), in which the route changes. All international calls are sent to the VoIP carrier DF in the default configuration. Digit collection is actived. In the time span for [Night1], these international calls are routed to VoIP carrier Ni, and in the time span for [Night2] they are routed through the PRI controller to the carrier with the prefix 010xx. National calls are always sent to VoIP carrier DF and local calls are routed to the outside line.

Example:

```
[System]
MapAll00=|40DF:00<<24
MapAll0=|40DF:0<<24
MapAll?=9?

[Night1]
MapAll00=|40Ni:00<<24
MapAll0=|40DF:0<<24
MapAll?=9?

[Night2]
MapAll00=9010xx00
MapAll0=|40DF:0<<24
MapAll?=9?
```

Any defined Night configurations must be set in the files pabx.cfg and route.cfg. If there are no changes in these sections, you must copy them from the System section. The complete Subscriber section must appear in the Night section of the pabx.cfg (see Chapter 5.2.5 on page 75 ⇨). The active route must appear in the route.cfg (see Chapter 5.3 on page 76 ⇨).

5.3.2 VOIP PROFILES

This section includes all of the most important parameters for communication with the VoIP peer.

Basic Parameters

Table 5.21 route.cfg: VoIP Basic Parameters

VoIP Basic Parameters
[Voip:<name>] Name of the routing profile. The name must begin with a letter and should be short and meaningful.
VoipDirection=<mode> Defines the direction in which VoIP calls can be set up. Possible options: In, Out, IO, None).
VoipPeerAddress=<ip addr> or <name> The peer's IP address or name. Default is 0 (if it is not set, the parameter VoipIpMask should be set to 0x00000000).
VoipIpMask=<ip mask> The subnetmask is used to determine the size of the IP address range for incoming traffic. The syntax is 0x followed by the mask in hexadecimal notation. Example of a Class C mask entry: 0xffffff00. Default is 0xffffffff (only incoming traffic is accepted from the defined peer address).
VoipSignalling=<int> Determines the profile's signaling protocol for outgoing VoIP calls. In the case of incoming calls, autorecognition ensures that each call from the peer is accepted, regardless of the protocol: 0=H.323 (default), 1=SIP udp, 2=SIP tcp.

Table 5.21 route.cfg: VoIP Basic Parameters *(continued)*

VoIP Basic Parameters
VoipCompression=<list> The compression to be used, in order of preference. At least one matching codec with the peer must be defined. Voice: g729, g729a, g729b, g729ab These codecs have a bit rate of 8 kbit/s (compression ratio 1:8). A stands for Annex A and B for Annex B. g72616, g72624, g72632 These ADPCM codecs have various bit rates: g72616 = 16kBit/s (compression ratio 1:4), g72624 = 24kBit/s and g72632 = 32kBit/s (compression ratio 1:2). **NOTE: G726 32kBit/s can also be signaled as G.721 by using the entry g721.** g728 The Codec has a bit rate of 16kBit/s (compression ratio 1:4). g711a, g711u These PCM codecs have a bit rate of 64kBit/s. No voice compression occurs. a stands for a-law and u for µ-law. g723, g723L These codecs work with 30ms data frames. g723.1 uses a bit rate of 6.3 kbit/s, and g723L uses a bit rate of 5.3 kbit/s to send RTP packets. **NOTE: This has no influence on the compression ratio of incoming RTP packets. Both sides must be able to receive both ratios.** gsm GSM-FR (full rate) has a bit rate of 13 kbit/s. The following codecs are also possible: g721 (SIP only) Fax: t38 T.38 (fax over IP) allows the transfer of fax documents in real time between 2 fax machines over IP. Following fax detection during a call, the voice codec will switch to T.38. Data: trp Transparent or clear mode (RFC 4040). Transparent relay of 64 kbit/s data streams. gnx64: Clear channel codec ccd: Clear channel data (as per RFC3108) Define a special profile for data call origination or destination numbers. Bear in mind that echo cancelation in this VoIP profile might be switched off (VoipECE=no).

Table 5.21 route.cfg: VoIP Basic Parameters *(continued)*

VoIP Basic Parameters
VoipMaxChan=<count> Maximum number of channels that can be used with the profile. If this parameter is not defined (default), there will be no limit. **NOTE: For versions 13.0c or lower, we recommend that you also set the parameter `VoipDelayDisc` to Yes to improve the ASR.**
VoipSilenceSuppression=<mode> Yes (default) activates silence suppression, CNG (comfort noise generation) and VAD (voice activity detection). No deactivates silence suppression. **NOTE: In SIP signaling, silence suppression is negotiated as per RFC3555.**
VoipTxM=<num> or <list> fix The multiplication factor (1-12) for the frame size for transmission of RTP packets (default is 4). 10ms is the default frame size (20ms for iGATE32). A list can be defined if different frame sizes are to be used for different codecs in the VoIP profile. The list must correspond with the list in the parameter VoipCompression. Normally the peer's frame size will be used if it is smaller than the one defined. If you enter fix, the configured factor will always be used.

Please refer to Chapter 9 ➩ for information on other possible entries.

Management Parameters

Table 5.22 route.cfg: VoIP Management Parameters

VoIP Management Parameters
VoipGk=<list> Name of the assigned gatekeeper profile. You can assign a profile to several gatekeepers to define backup gatekeepers for a VoIP profile. In this case, the next gatekeeper will be used if the previous one fails.
VoipProxy=<ip addr> Enter the IP address of the SIP server.
VoipUser=<username> Define the username for the remote device if authentication is required (SIP only).
VoipPwd=<password> Define the password for the remote device if authentication is required (SIP only).
VoipRegistrar=<name> Enter the name of a registrar to be used for the VoIP profile.
VoipRadiusAuthenticate=<name> Enter the name of the Radius server to activate user authentication.
VoipRadiusAccounting=<name> Enter the name of the Radius server to activate accounting.
VoipIpLogging=<mode> Enter Yes to activate recording IP addresses in the CDRs (default is No). The first IP address is the signaling address and the second is the RTP address, followed by the the codec and the frame size used. . The IMSI appears after the IP addresses if the keyword IMSI is defined in the pabx.cfg. Example of a CDR entry: 21.08.07-11:01:42,21.08.07-11:01:58,40,912345,192.168.0.2:192.168.0.2,G729,10,0101,16,10,0 Example of a failed log entry: 21.08.07-11:11:30,40,91234,192.168.0.2:192.168.0.2,G729,10,0101,ff,2,1

5.3.3 GATEKEEPER PROFILES

Gatekeeper profiles are used to connect the iGATE to several systems by using a gatekeeper if the protocol is H.323. It is possible to configure different gatekeepers for different destinations and to define backup gatekeepers.

These gatekeeper profiles are then assigned to the VoIP profiles:

Table 5.23 route.cfg: Gatekeeper Parameters

Gatekeeper Parameters
[Gatekeeper:<name>] Name of the gatekeeper profile.
RasPort=<port> Indicates the port the gatekeeper uses (default 1719) for registration, admission and status.
OwnRasPort=<port> Indicates the port the system uses (default 1719) for registration, admission and status.
RasPrefix=<list> iGATE's defined prefix(es). Use a space to separate entries.
RasId=<name> The alias used for gatekeeper registration.
GkId=<name> The gatekeeper's alias.
GkPwd=<name> Password to log onto the gatekeeper. If you do not use authentication, leave this entry blank.
GkAdd=<ip addr> The gatekeeper's IP address.
GkTtl=<sec> Gatekeeper time to live (default 0 means infinite).
GkMaxChan=<count> Max. number of channels used for this gatekeeper. If this parameter is not defined (default), there will be no limit.

Table 5.23 route.cfg: Gatekeeper Parameters *(continued)*

Gatekeeper Parameters
GkDynMaxChan=<mode> The static number of available channels in the gatekeeper profile (GkMaxChan=<count>) is replaced with a dynamic number of active mobile ports (up to the number entered in GkMaxChan) when Yes is entered here. Default is No.
GkUseStun=<mode> Enter yes (default) to use the STUN values for the GK profile.
GkTerminalAliasWithPrefix=<mode> Some gatekeepers may require that prefixes are listed in the Terminal Alias section. Enter Yes to activate this function; default value is No).
GkTerminalTypeWithPrefix=<mode> Enter no to deactivate sending the Dialed Prefix Information in the Registration Request (default yes).

5.3.4 REGISTRAR PROFILES

Registrar profiles are used to register the iGATE with a SIP registrar. It is possible to configure different registrars for different destinations and to define backup registrars. These registrar profiles are then assigned to the VoIP profiles:

Table 5.24 route.cfg: Registrar Parameters

Registrar Parameters
[Registrar:<name>] The name of the registrar profile.
RegId=<name or ip addr> Host name or IP address used in the register's request header. Bear in mind that the DNS service must be active if you enter the host name.
RegOwnId=<name@ip addr/domain> Typically a host name or telephone number followed by an @ sign and a domain name or IP address. The entry used in the `From:` field. The default setting is `RegUser@RegId`.
RegContact=<name or ip addr> Used in the `Contact:` field.
RegUser=<name> Enter a username for authorization.

Table 5.24 route.cfg: Registrar Parameters *(continued)*

Registrar Parameters
RegPwd=<password> Enter a password for authorization.
RegProxy=<ip addr> Enter an alternative IP address if you want the request to be sent to an address other than the one entered in `RegId`.
RegExpires=<sec> Enter the number of seconds registration is to be valid. Default `0` means infinite.
RegPing=<sec> Interval (in seconds) for the registrar ping. The iGATE sends an empty UDP packet to the registrar's IP address. The packet is essentially an alive packet to avoid possible firewall problems.

5.3.5 RADIUS PROFILES

Radius profiles are used to connect the iGATE to a Radius server. You can use a Radius server for different destinations and for access and/or accounting. These Radius profiles are then assigned to the VoIP profiles:

Table 5.25 route.cfg: Radius Parameters

Radius Parameters
[Radius:<name>] The name of the Radius server profile assigned to one or more VoIP profiles.
Host=<name or ip addr> Radius server's host name or IP address. Bear in mind that the DNS service must be active if you enter the host name.
User=<name> Enter a username for authorization.
Password=<password> Enter a password for authorization.
Secret=<secret> Enter the shared secret.
OwnId=<name or ip addr> Host name or IP address used in the NAS identifier or NAS IP address (Cisco VSA gateway ID).
ServiceType=<num> As defined in RFC 2865, Chapter 5.6.

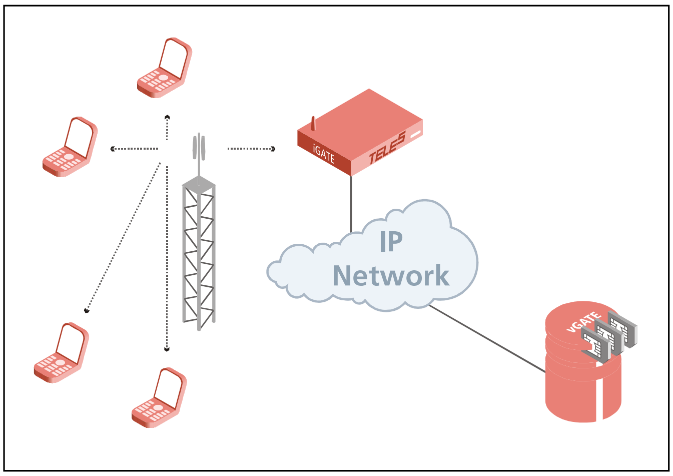
Table 5.25 route.cfg: Radius Parameters *(continued)*

Radius Parameters
RequestTimeout=<sec> Number of seconds during which the request is repeated if the Radius server does not respond.
RequestRetries=<count> Number of packet retries sent at one time.
StopOnly=<mode> When `yes` is entered, only Accounting Request Messages with the status type `stop` are transmitted to the Radius server.
AlwaysConnected=<mode> Enter `No` (default) to set the value for the field `ConnectedTime` to that of the field `DisconnectedTime` in accounting-stop messages when the call was not connected.
CallingStationId=<num> This parameter is used to set the calling station ID. The default setting is the OAD, but you can define any calling station ID. To define a partial calling station ID, enter a `?` for each digit. For example, `CallingStationId=???` will consist of the first three digits of the OAD.
CallType=<int> Enter one of the following to define the call type: 3 = VoIP and telephony 2 = VoIP only 1 = Telephony only
FramedProtocol=<int> Enter one of the following to define the framed protocol (see RFC 2865, Chapter 5.7): 1 = PPP 2 = SLIP 3 = AppleTalk Remote Access Protocol (ARAP) 4 = Gandalf proprietary SingleLink/MultiLink protocol 5 = Xylogics proprietary IPX/SLIP 6 = X.75 Synchronous
NasId=<string> The string entered is used as network access server identifier attribute in access requests. If no string is entered, the attribute will not be set (default).

6 ROUTING EXAMPLES

6.1 IGATE INTEGRATION IN A CARRIER NETWORK

The parameter `VoipUseIpStack` must be set in the VoIP profile.



In the following example, a iGATE32 is integrated in a carrier network via DSS1. It is connected to a vGATE and receives SIM-card information from a centralized SIM-card server. The IP address for the vGATE Control Unit is 172.16.0.100. The parameter `SIMS` is used in `SIM<x>` to connect the mobile controller with the vGATE. All calls coming from ISDN are sent to two different mobile networks: Calls with the prefixes 01555 and 01556 are sent to the carrier with the LAIN 26212 at controllers 0-15. Calls with the prefixes 01444 and 01445 are sent to the carrier with the LAIN 26313 (controllers 16-31). Digit collection is activated, so that incoming calls with overlap dialing are not transmitted until the number is complete or a wait timer (5 seconds) has run out. The `NEXT` parameter makes sure that calls are distributed evenly to the individual mobile channels in the trunk group. The parameter `CHADDR` ensures that calls are not misrouted, since the controller definition changes to the SIM-card's LAIN when a SIM card is mistakenly used for another mobile controller. Problems can occur when SMS messages are also sent, as service center numbers are definitively configured.

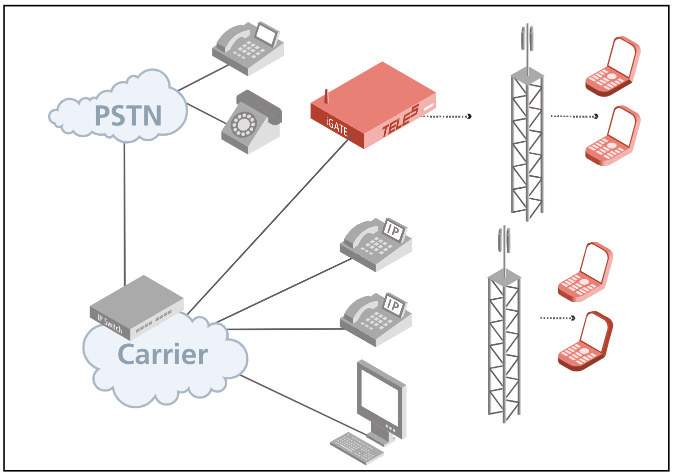
Configuration in the pabx.cfg

```
Subscriber00 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIMS,IMSI] CHADDR ALARM NEXT
Subscriber01 = TRANSPARENT ROUTER GSM[0000,00000,+491555555,1,1,1,SIMS,IMSI] CHADDR ALARM
....
Subscriber16 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIMS,IMSI] CHADDR ALARM NEXT
Subscriber17 = TRANSPARENT ROUTER GSM[0000,00000,+491666666,1,1,1,SIMS,IMSI] CHADDR ALARM
....
Subscriber32 = TRANSPARENT ROUTER ALARM
Subscriber33 = TRANSPARENT ROUTER ALARM

SimCtrlUnitAddress=172.16.0.100
```

Configuration in the route.cfg

```
[System]
DTMFWaitDial=5

MapAll01555=|2621201555<<17
MapAll01556=|2621201556<<17

MapAll01444=|2621301444<<17
MapAll01445=|2621301445<<17
```

6.2 IGATE INTEGRATION WITH SIM-CARD SWITCHING IN AN H.323 CARRIER NETWORK



In the following example, a iGATE32 is integrated in a carrier network via H.323. The system contains six SIM cards for each mobile channel, and the SIM 24 Carrier is used. All calls coming from VoIP are routed to the mobile network. Four VoIP Modules with 16 media channels each are attached in the system. H.323 is used as the signaling protocol and a gatekeeper is used in the VoIP network. Because the gatekeeper assigns and authorizes the peer, only one VoIP profile is necessary. Since the peers may use various compression algorithms, you can define several if you so choose. The codec with the highest priority is G.729. If the peer does not support it, G.726 32Bit/sec, G.711a, G.711u are also possible. Silence suppression is active. The gatekeeper's IP address is 192.168.0.10. This gatekeeper profile can handle up to 30 simultaneous VoIP calls. This value is dynamic and changes depending on the number of active SIM cards. The iGATE's alias is iGATE01. The prefix list is 01555 01556 01444 01445. The gatekeeper's alias is GK1 and no password is used. Calls with the prefixes 01555 and 01556 are sent to the carrier with the LAIN 26212 at controllers 0-15. Calls with the prefixes 01444 and 01445 are sent to the carrier with the LAIN 26313 (controllers 16-31). Digit collection is activated, so that incoming calls with overlap dialing are not transmitted until the number is complete or a wait timer (5 seconds) has run out. The `NEXT` parameter makes sure that calls are distributed evenly to the individual mobile channels in the trunk group. The parameter `CHADDR` ensures that calls are not misrouted, since the controller definition changes to the SIM-card's LAIN when a SIM card is mistakenly used for another mobile controller. Problems can occur when SMS messages are also sent, as service center numbers are definitively configured. The parameter `LIMIT` is set so that the system automatically switches to the mobile controllers' SIM cards when the active SIM card has been used for 3600 seconds. The parameter `CONTINUE` makes sure the mobile channel switches to the first SIM card after the limit has been reached on the last SIM card. The SIM card will not switch until currently active calls have been disconnected.

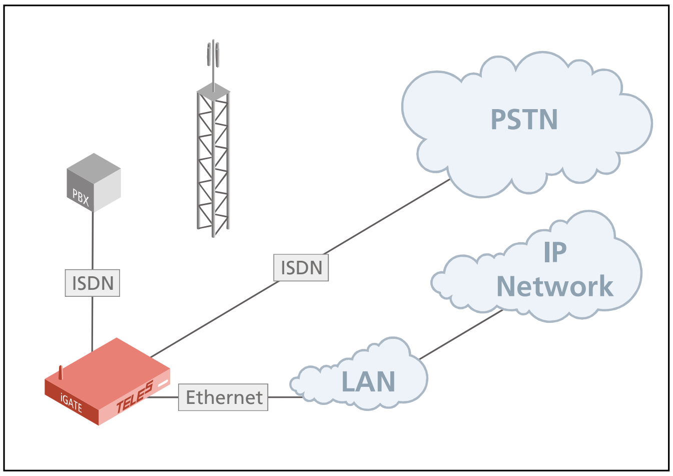
Configuration in the pabx.cfg

```
Subscriber00 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24,IMSI] CHADDR LIMIT[3600] CONTINUE
ALARM NEXT
Subscriber01 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24,IMSI] CHADDR LIMIT[3600] CONTINUE
ALARM
....
Subscriber16 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24,IMSI] CHADDR LIMIT[3600] CONTINUE
ALARM NEXT
Subscriber17 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24,IMSI] CHADDR LIMIT[3600] CONTINUE
ALARM
....
Subscriber34 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
Subscriber35 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
Subscriber36 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
Subscriber37 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
ChargeUnitGenerate=1
LimitWODisc=ON
```

Configuration in the route.cfg

```
[System]
DTMFWaitDial=5

MapAll01555=|2621201555<<17
MapAll01556=|2621201556<<17

MapAll01444=|2621301444<<17
MapAll01445=|2621301445<<17

[Voip:DF]
VoipDirection=In
VoipPeerAddress=10.0.0.0
VoipIpMask=0xffff0000
VoipSignalling=0
VoipCompression=g729 g72632 g711a g711u
VoipSilenceSuppression=Yes
VoipMaxChan=30
VoipTxM=2
VoipGk=GK1

[Gatekeeper:GK1]
RasPort=1719
OwnRasPort=1719
RasId=iGATE01
RasPrefix=01555 01556 01444 01445
GkId=GK
GkAdd=192.168.0.10
GkPwd=
GkTtl=300
GkMaxChan=30
GkDynMaxChan=Yes
```

6.3 IGATE AS A SECOND-GENERATION LCR WITH VOIP



In the following example of a PBX connection, all mobile calls are terminated through the mobile channels. Eight mobile channels form a group for one mobile network. One SIM card is available on each mobile channel. Digit collection is activated, so that incoming calls with overlap dialing are not transmitted until the number is complete or a wait timer (5 seconds) has run out. The `NEXT` parameter makes sure that calls are distributed evenly to the individual mobile channels in the trunk group. If all of a carrier's SIM cards are busy, rerouting (`redirect3`) via PSTN is automatically initiated. All international calls are terminated to VoIP (40). The system contains two VoIP Modules, for a total of 32 media channels. The VoIP carrier profile `DF` and the SIP protocol are used. National calls are routed through the carrier with the prefix 010xx. All other calls are sent to the PSTN unchanged. All calls from the PSTN or from a VoIP carrier are sent directly to the NT controller, to which the PBX is attached. All incoming calls from the mobile networks are routed to the PBX's central number (001). For the VoIP profile `DF`, the system uses the registrar `reg` and registers with `user@sip-carrier.de`, username `user` and password `pwd`. SIP UDP is used for signaling. A maximum of 30 media channels with the G.729 codec can be used. The Peer is `sip-carrier.de`.

Configuration in the pabx.cfg

```
Subscriber00 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4,IMSI] CHADDR ALARM NEXT
Subscriber01 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4,IMSI] CHADDR ALARM
....
Subscriber08 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4,IMSI] CHADDR ALARM NEXT
Subscriber09 = TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4,IMSI] CHADDR ALARM
....
Subscriber16 = TRANSPARENT ROUTER ALARM
Subscriber17 = TRANSPARENT ROUTER ALARM
Subscriber18 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
Subscriber19 = TRANSPARENT ROUTER SWITCH CHMAX[16] ALARM
```

Configuration in the route.cfg

```
[system]
DTMFWaitDial=5

Restrict9=10
Restrict40=10
Restrict26212=10001
Restrict26213=10001

MapOut01555=|2621201555<<17
MapOut01556=|2621201556<<17
MapOut01666=|2621301666<<17
MapOut01665=|2621301665<<17
MapOut00=40DF:00
MapOut0=010xx0
MapOut?=9?

Redirect326212=A
Redirect326213=A
MapAllA=9

[Voip:DF]
VoipDirection=IO
VoipPeerAddress=sip-carrier.de
VoipIpMask=0xffffffff
VoipSignalling=1
VoipCompression=g729 t38
VoipSilenceSuppression=Yes
VoipMaxChan=60
VoipTxM=4
VoipOwnAddress=user@sip-carrier.de
VoipUser=user
VoipPwd=pwd
VoipRegistrar=reg

[Registrar:reg]
RegId=sip-carrier.de
RegOwnId=user@sip-carrier.de
RegContact=user@sip-carrier.de
RegUser=user
RegPwd=pwd
```

7 MOBILE CONFIGURATION OPTIONS

Be sure to save a backup copy of the configuration files before making changes. Changing configuration data and/or SIM-card positions may lead to malfunctions and/or misrouting, as well as possible consequential damages. Make changes at your own risk. TELES is not liable for any damages resulting from or related to such changes. Therefore, please thoroughly check any configuration changes you or a third party have made.

7.1 CONNECTION TO A VGATE

The vGATE is a system that enables more convenient management of a network of iGATE systems. All SIM cards in the network are installed in and maintained at a central server, so that it is no longer necessary to install SIM cards into each gateway. The iGATEs connected to the vGATE do not require SIM-card carriers, as the vGATE contains SIM-card carriers for the entire network.

Bear in mind that no SIM-card carriers are to be inserted in iGATEs connected to a vGATE.

The following parameters must be configured in the `pabx.cfg` of each iGATE connected to the vGATE. After the parameters have been entered, you must restart the iGATE to activate the changes:

SIMS

Enter this keyword in the `Subscriber` lines of the mobile controllers to connect the system to a vGATE.

EXAMPLE:

```
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIMS] CHADDR ALARM
```

SimCtrlUnitAddress=<ip addr>

Enter the vGATE Control Unit’s IP address. Set this parameter in the IP configuration section.

EXAMPLE:

```
SimCtrlUnitAddress=192.168.0.1
```

7.2 MODULE DISTRIBUTION OF VARIOUS MOBILE NETWORKS

You can assign each mobile port in the iGATE system either one mobile network or different access groups to different mobile networks. The port numbers in the iGATE must be the same for the individual groups.

The keyword NEXT ensures equal distribution of calls.

The following configuration samples (from the `pabx.cfg` configuration file) show the changes:

Example 1 All ports in the following example must have the same number for all mobile channels to route calls to the same mobile network. The `subscriber` line of the first port must also contain the keyword NEXT to ensure the equal distribution of calls.

```
...
Controller00=20 GSM
Controller01=20 GSM
Controller02=20 GSM
Controller03=20 GSM
Controller04=20 GSM
Controller05=20 GSM
Controller06=20 GSM
Controller07=20 GSM
Controller08=20 GSM
Controller09=20 GSM
Controller10=20 GSM
Controller11=20 GSM
Controller12=20 GSM
Controller13=20 GSM
Controller14=20 GSM
Controller15=20 GSM
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM NEXT
Subscriber01=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber02=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber03=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber06=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber07=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber08=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber09=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber10=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber11=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
...
```

Example 2 In the following example, a group of 16 mobile channels is assigned to three different mobile networks. The `subscriber` line of the first port in each group must contain the keyword NEXT to ensure the equal distribution of calls.

```
...
Controller00=20 GSM
Controller01=20 GSM
Controller02=20 GSM
Controller03=20 GSM
Controller04=20 GSM
Controller05=20 GSM
Controller06=22 GSM
Controller07=22 GSM
Controller08=22 GSM
Controller09=22 GSM
Controller10=22 GSM
Controller11=22 GSM
Controller12=24 GSM
Controller13=24 GSM
Controller14=24 GSM
Controller15=24 GSM
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM NEXT
Subscriber01=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber02=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber03=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber06=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM NEXT
Subscriber07=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber08=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber09=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber10=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber11=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM NEXT
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] ALARM
...
```

7.3 NETWORK-SPECIFIC MOBILE ROUTING

7.3.1 USING A FIXED MOBILE PORT ADDRESS

The customer's network routes calls to the mobile network with a defined prefix. Because this code is not always uniform, the iGATE might have to convert it. Conversion requires the following information:

- The mobile network's access number
- Destination number format (with or without prefixes, national or international)

Conversion occurs according to the following formula:

```
<national/international><prefix[incoming]>=<destination number>
```

converted as:

```
<port><mobile network access number><destination number>
```

Be sure to make the following entry in the route.cfg configuration file to configure this conversion:

```
MapAll<nat./int.>prefix[incoming]>=<port><mobile network access number>
```

The iGATE system converts national into one zero and international into two zeros.

The following configuration exemplifies this conversion as it might occur in Germany:

```
...
MapAll00491555=2001555
MapAll00491556=2101556
...
```

This example shows how the customer's network provides the prefix international+49+1555+destination number for one mobile network, and international+49+1556 for the other. The configuration entries see to it that 00491555+destination number is converted to 2001555+destination number and 00491556+destination number is converted to 2101556+destination number. The calls to the carrier with prefix 01555 are routed to ports with the number 20 and calls to the carrier with prefix 01556 are routed to the ports with the number 21.

7.3.2 USING THE LAIN AS THE MOBILE PORT ADDRESS

Use the LAIN as controller with the CHADDR parameter to prevent logging onto the wrong SIM card. This will ensure that routing is network specific. The following example is based on the German country code. One carrier's LAIN is 26212 and the other carrier's LAIN is 26213:

pabx.cfg

```
...
Controller00=20 GSM
Controller01=20 GSM
Controller02=20 GSM
Controller03=20 GSM

Controller04=20 GSM
Controller05=20 GSM
Controller06=20 GSM
Controller07=20 GSM
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+49556,1,1,1,SIM4] CHADDR ALARM
Subscriber01=TRANSPARENT ROUTER GSM[0000,00000,+49556,1,1,1,SIM4] CHADDR ALARM
Subscriber02=TRANSPARENT ROUTER GSM[0000,00000,+49556,1,1,1,SIM4] CHADDR ALARM
Subscriber03=TRANSPARENT ROUTER GSM[0000,00000,+49556,1,1,1,SIM4] CHADDR ALARM

Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM4] CHADDR ALARM
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM4] CHADDR ALARM
Subscriber06=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM4] CHADDR ALARM
Subscriber07=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM4] CHADDR ALARM
...
```

If you remove the keyword CHADDR from the `pabx.cfg`, you must restart the system. Controllers belonging to the same trunk group must have the same address. You must delete all routing entries based on port addresses when using the LAIN as controller.

route.cfg

```
...
MapAll01555=2621201555
...
MapAll01556=2621301556
...
```

7.3.3 FIXED LAIN FOR A MOBILE PORT

Enter `CHADDR[<addr>]` to remove a mobile controller belonging to an LAIN group from the standard routing process (e.g. for specific routes or only for SMS transmission). The port address can be set to `<addr>`.

Example:

```
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM4] CHADDR[444] ALARM

MapAllSMS=444 05
```

7.4 INCOMING VOICE CALLS FROM MOBILE

Incoming mobile calls (service indicator 01 represents voice calls) can be routed to a specified number. This enables each mobile controller to receive a unique identifier. It will then be mapped to a number:

```
Restrict20=90123 01
Restrict21=91234 01
```

The mobile controllers can also have the same identifier, so that all voice calls (service indicator 01) from controller 20 are sent to number 1111 at port 9. This number could, for example, serve a call center.

```
Restrict20=91111 01
```

7.5 BLOCKING PORTS

This function allows you to block a port, so that the corresponding mobile channel is omitted from the distribution of calls. The function is particularly useful when mobile channels fail or SIM cards cannot be immediately replaced.

To block a port (i.e. a mobile channel), enter the keyword CHINC[...] in the Subscriber line.

In Example 1 ➪, port 10 is blocked.

Example 1

```
...
Subscriber10=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM4] CHADDR ALARM CHINC[01,01]
...
```

To activate the port, remove the entry and enter **Activate configuration**.

It is also possible to block an entire port with the remote administration program GATE Manager. The CHINC[...] function is not necessary with this application. The port's status is displayed by remote administration. You can remove the block with **Activate a configuration** or with the **Unblock** option.

7.6 SETTING LIMITS

This function enables you to monitor time units. A unit can be set, either to the defined time interval or in 10-second intervals (default value). At the beginning of the defined unit, the current connection is torn down either immediately or when the call has been terminated (cf. Chapter 7.7.3 on page 102 ⇨); no more connections will be set up. An alarm also goes off and an entry is generated in the log file.

Bear in mind that you must add 1 to the values you wish to set, since the units change at the beginning of each interval.

Setting SIM Time Limits

In the following example, the mobile channel shuts down at the beginning of the last 10-second unit of 6,001:

```
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4] CHADDR ALARM NEXT LIMIT[6001]
...
```

Setting the Default Time Window

In the following example, the mobile channel shuts down when a calculated number of units set in LIMIT has commenced. If ChargeUnitGenerate=<sec> is configured, the mobile channel will shut down at the beginning of the last unit entered in LIMIT multiplied by the value entered here. The default value for this parameter is 10 seconds. Bear in mind that the value entered in LIMIT may not exceed 65535. In the example, the mobile channel will shut down at 60,000 seconds.

```
...
ChargeUnitGenerate=1
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM4] CHADDR ALARM NEXT LIMIT[60001]...
```

Setting Start Units

The following example shows how you can use the keyword ChargeUnitFirst=<seconds> to configure a starting unit for LIMIT. The following entries are used for SIM card rates where the first defined number of seconds are always charged (e.g. the first minute). After this initial number of seconds has passed, the subsequent charges will be calculated in intervals defined by `ChargeUnitGenerate` (e.g. every 10 seconds):

```
...
ChargeUnitFirst=60
ChargeUnitGenerate=10
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24] LIMIT[6061] ALARM NEXT...
...
```

Information about the active SIM cards can be found in GATE Manager and **Port Status**.

To remove limits from the configuration, follow these steps:

- Enter LIMIT[-].
- Activate the configuration.
- Delete the entry LIMIT[-].
- Activate the configuration again.

7.7 AUTOMATIC SIM SWITCHING

This function enables you to monitor time quotas. A limit can be set, either to the defined time interval or in 10-second intervals (default value). When this value is reached, the current connection is torn down either immediately or when the call has been terminated; either no more connections will be set up or the system will switch to another SIM card. An alarm also goes off and an entry is generated in the log file.

You can configure different limits for each SIM card per mobile channel. To activate this function, enter the keyword LIMIT[<val1>,<val2>,<val3>,<val4>,<val5>,<val6>] at subscriber for the corresponding port. <valx> defines a number of units as a threshold value for the respective SIM card. If only one limit is entered, this limit will apply for all SIM cards at this port.

Make sure the SIM24 card carrier is inserted and the size of the SIM-card carrier (SIM24) is entered in the `Subscriber` line.

If a dash (-) is entered for <valx>, no limit will apply for the corresponding SIM card. If only two values are entered, a dash must be entered for the other SIM cards; these SIMs will have no limit. A corresponding alarm message is generated when the limit on each card has been reached. If the keyword CHANGE is configured, the mobile channel **will not** switch beyond the sixth SIM card.

Different settings are possible for the various SIM-card carriers. The number entered (4, 24) refers to the number of slots. The respective number of SIMs per mobile channel is 1 or 6.

The following configurations are possible. Settings shown here are for the SIM-24 carrier:

Table 7.1 SIM Switching Configurations

Configuration	Definition
LIMIT[10,20,30,40,10,20] CHANGE	Each SIM card has a defined limit.
LIMIT[10] CHANGE	Each SIM has the same limit.
LIMIT[10,-,-,-,-,-] CHANGE	The first SIM has a defined limit, the second has none.
LIMIT[10,20,0,0,10,20] CHANGE	SIMs 1, 2, 5 and 6 have defined limits. The SIMs in positions 3 and 4 are not used.

If the keyword CONTINUE is configured, the mobile channel will switch beyond the sixth SIM card. When the limit on the last card has been reached, the mobile channel will switch back to the first card.

7.7.1 SWITCHING SIMS

In the following example, the mobile channel shuts down and switches to the next SIM card when 6,000 intervals of 10 seconds each have passed. The port is blocked after the limit has been reached on the last SIM card:

```
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NEXT LIMIT[6000] CHANGE...
```

7.7.2 CYCLICAL SIM SWITCHING

In the following example, the mobile channel shuts down and switches to the next SIM card when 6,000 intervals of 10 seconds each have passed. The mobile channel switches to the first SIM card after the limit has been reached on the last SIM card. To reset the counter on a monthly basis, see Chapter 11.4.1 on page 208 ➪:

```
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NEXT LIMIT[6000] CONTIN-
UE...
```

In the following example, only two SIM cards are inserted in the SIM-card carrier. These SIMs are used alternately in intervals of 3600 seconds each:

```
...
ChargeUnitGenerate=1
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NEXT
LIMIT[3600,3600,0,0,0,0] CONTINUE...
```

7.7.3 IMMEDIATE SIM SWITCHING

In the following example, the mobile channel shuts down after the call has been disconnected, and switches to the next SIM card when 6,000 intervals of 10 seconds each have passed. When the parameter LimitWODisc is ON, the call will be torn down when the calling party hangs up. If it is set at OFF, the call will be terminated immediately when the limit is reached:

```
LimitWODisc=OFF
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NEXT LIMIT[6000] CHANGE...
...
```

7.7.4 COUNT STATUS INFORMATION

To find information about the current counts and limits for each mobile channel, click **Statistics** in the GATE Manager.

For mobile ports:

- **Count A-F** For each mobile channel. Counts are the time slices (from 0 to the limit value) for the individual SIM cards (1-6). When a SIM's set time limit is reached, the channel will disconnect and the next SIM will log on.
- Click **Reset/Set** Counters in the **Statistics** context menu in GATE Manager to reset the counters (default value is 0). You can also configure the counters to reset automatically (cf. Chapter 11.4.1 on page 208 ⇨).

If `LIMIT` is configured, bear in mind that SIM 1 must be configured in the `pabx.cfg` for the corresponding mobile port.

7.8 DEFINING TIME LIMITS FOR CALLS

By entering the parameter CALL in the Subscriber line, you can terminate calls that reach a defined time limit. For each call the limit is reset at 0. You can define a value anywhere within <limit>-<random>, and you can define a maximum value for <random>. The value entered for CALL must be at least 30 seconds.

Bear in mind that you must add 1 to the values you wish to set, since the units change at the beginning of each interval

If this parameter is configured once, it will be set in each configuration file. If you prefer not to use it for all SIMs, set the limit higher than any call is likely to last (e.g. 360,000 seconds). To deactivate this function, remove the entry from the pabx.cfg and restart the system.

Example:

```
ChargeUnitGenerate=1;defines the factor for the limit entry (600*1=600sec)
ChargeUnitDivisor=5 ;random value that defines the maximum call duration between 595 and 600secs
...
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,+000000,1,1,1,SIM24] CALL[601]
```

The following entry is required if the iGATE is used in conjunction with a vGATE:

```
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,+000000,1,1,1,SIMS] CALL[600]
```

This function cannot be used in conjunction with the `LIMIT` function described in Chapter 7.7 ⇨.

7.9 PAUSE BETWEEN TWO CALLS

If the parameter WAIT appears in the Subscriber line, the mobile controller will not be used after a successful connection for a random amount of time between 1 and 30 seconds

Example:

```
Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIM24,IMSI] CHADDR WAIT ALARM
```

7.10 TIME-CONTROLLED SIM SWITCHING

You can define a time at which a mobile channel will change to another SIM card (up to six SIM cards are possible for this option). Before proceeding, please refer to Chapter 5.2.1.3 ⇨ for basic information.

You must define all time windows you would like to use in the [System] section of the pabx.cfg, in the subsection night configuration.

The following entry in the configuration file pabx.cfg is necessary:

`Night<num>=<time> <day>`

Example: In the following example, six time windows are defined. The standard configuration is active every day from 12:00 midnight to 4:00 a.m.. The time window `Night1` is active from 4:00 to 8:00 a.m., etc.

```
;Night configuration
; ---------------------
Night1=04:00 11111111
Night2=08:00 11111111
Night3=12:00 11111111
Night4=16:00 11111111
Night5=20:00 11111111
NightResetTime=00:00 11111111
```

To generate a NightConfiguration section for SIM switching, copy the complete Subscriber subsection from the [System] section after making the appropriate entries in the [Nightx] section.

Finally, enter the SIM-card number (1-6 for the SIM 24 Carrier) that is to be active during the specified time period in the mobile port's subscriber entry.

Example: In the following example, SIM cards change in the individual time windows (as configured above). Only the `Subscriber` lines for controllers 12-15 are presented in simplified form. In a proper configuration, all `Subscriber` lines must be defined.

```
[System]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,1,1,1,SIM24] ALARM
...
[Night1]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,2,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,2,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,2,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,2,1,1,SIM24] ALARM
...
[Night2]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,3,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,3,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,3,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,3,1,1,SIM24] ALARM
...
[Night3]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,4,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,4,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,4,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,4,1,1,SIM24] ALARM
...
[Night4]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,5,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,5,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,5,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,5,1,1,SIM24] ALARM
...
[Night5]
...
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,+49555,6,1,1,SIM24] ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,+49555,6,1,1,SIM24] ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,+49555,6,1,1,SIM24] ALARM
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,+49555,6,1,1,SIM24] ALARM
...
```

The only difference is in the active SIM card. Activate the configuration after the required files have been copied onto the system.

Bear in mind, that you must also make the appropriate entries in the corresponding route.cfg sections. For more information, please refer to Chapter 5.3 ⇨.

This function cannot be used in conjunction with the `LIMIT` function described in Chapter 7.7 ⇨.

Time-Controlled Logoff of a Mobile Channel or SIM Card

If a dash (`-`) is entered in the SIM-card position, the SIM card will log off automatically. Time-controlled activation of configuration files makes it possible to shut off unneeded SIMs, for example at night.

Example:

```
[System]
Subscriber12=ALARM GSM[0000,00000,+49555,1,1,1,SIM24]
Subscriber13=ALARM GSM[0000,00000,+49555,1,1,1,SIM24]
Subscriber14=ALARM GSM[0000,00000,+49555,1,1,1,SIM24]
Subscriber15=ALARM GSM[0000,00000,+49555,1,1,1,SIM24]
[Night1]
Subscriber12=ALARM GSM[0000,00000,+49555,2,1,1,SIM24]
Subscriber13=ALARM GSM[0000,00000,+49555,2,1,1,SIM24]
Subscriber14=ALARM GSM[0000,00000,+49555,2,1,1,SIM24]
Subscriber15=ALARM GSM[0000,00000,+49555,2,1,1,SIM24]
[Night2]
Subscriber12=ALARM GSM[0000,00000,+49555,-,1,1,SIM24]
Subscriber13=ALARM GSM[0000,00000,+49555,-,1,1,SIM24]
Subscriber14=ALARM GSM[0000,00000,+49555,-,1,1,SIM24]
Subscriber15=ALARM GSM[0000,00000,+49555,-,1,1,SIM24]
```

7.11 MOBILE-USER PBX CALLBACK

When the iGATE is implemented in a corporate network and connected to a PBX or between a PBX and the outside line, the following configuration entry activates a feature, that uses a mobile caller’s OAD to connect with the last PBX extension the caller unsuccessfully dialed:

Callback is not possible for VoIP calls.

`DialBack=<hours>`

The callback list is active for the number of hours entered.

Example: In the following example, the callback list is active for the previous five hours. The German country code is used for the LAINs. All calls with the prefixes 1111 and 2222 are terminated through the carrier with the LAIN 26212. Calls with the prefix 3333 are terminated through the carrier with the LAIN 26213:

```
DialBack=5

MapAll1111=262121111
MapAll2222=262122222
MapAll3333=262133333
```

Make sure that no `Restrict` entries are configured for these mobile controllers.

7.12 OPTIONAL MOBILE QUALITY PARAMETERS

The following table describes specific signaling and quality parameters for configuration of the mobile interface.

Table 7.2 Optional Mobile Parameters

GSM=...	
Enter any of the following parameters after the equal sign for the following functions. Entries may appear in any order, but all entries must appear in the same line and in double-digit notation as follows: `GSM=RSSI[10] STOP[18,08] ANNOUNCE[00,08] FAX[a2] ASR[20,35]`	
ALERT[<sec>]	Set this parameter to generate alert signal in the D channel immediately after dial-end signal. If you enter optional square brackets containing a number of seconds, the alert signal will occur when the number entered has passed.
ANNOUNCE	Set this parameter to define what happens when a recorded announcement is recognized: ▪ No **`ANNOUNCE`** entry (default) A D-channel PROGRESS message stating Inband Information Available will be generated ▪ `ANNOUNCE[<cause>]` The connection will be rejected with the defined ISDN cause value. ▪ `ANNOUNCE[00,<sec>]` A timeout for voice recognition is defined in seconds (default value: 120 seconds). After the interval entered has passed, the connection is torn down.
ASR[<limit>, <calls>]	Allows you to change the default value (40 calls at 30% ASR). For a definition of ASR, see Chapter 11.4.1 ➪.

Table 7.2 Optional Mobile Parameters *(continued)*

GSM=...	
FAX[<cause>]	This entry allows you to reject fax calls with the defined cause value.
RSSI[<limit>]	Configure this parameter to set a limit for the reception field strength. When the reception field strength falls below this limit, the mobile channel will be blocked. If the field strength is above the limit, the mobile channel will log on with the mobile carrier again. The values used are 0 to 31, which represent the following field strengths: -113dBm to -51 dBm. An error is generated in the `protocol log`. The result must be divided by 2. EXAMPLE: To define a field strength of -95 dBm, subtract -95 from-113 and divide the result by 2: - 113dB - (-95dB) = -18dB / 2 = 9 Enter `RSSI[9]`
STOP[<val1>, <val2>]	This entry allows you to define a maximum number of connection setups that always result in a recorded message (<val1>) without a call-connected signal or successful connection setup, or that are always accepted (<val2>). The mobile port is blocked when the defined value is reached and an entry is recorded in the log file (...Err: Voice). In this way inactive SIM cards that are forwarded to a recording (with or without a connect from the mobile carrier) can be recognized and blocked so that they are removed from the routing process. The default status of this function is off.
NOCP	When this option is configured and the call is from ISDN to GSM, the Call Proceeding signaling message will be eliminated from signaling. This may be necessary if the ISDN peer does not support Call Proceeding. Bear in mind that the peer's Setup Ack Timer is usually set at 5 seconds, which means that an Alert must be generated as follows: `GSM=ALERT[5]`

7.13 DEACTIVATING CLASS 2 RE-ROUTING

Configuring Class2Next=Off in the pabx.cfg file ensures that calls rejected with a class 2 cause value are not re-routed to the next available port.

7.14 CHECKING PORTS/MOBILE CHANNELS

Monitoring ASR for Mobile Ports

ASR monitoring of the last 40 calls occurs for all mobile ports. If the ASR (ASR2) is lower than 30 percent, an alarm is generated at the corresponding port and the port is blocked. The port is then restarted and a corresponding entry appears in the protocol.log file (ASR). The port is then unblocked.

The following entry in the pabx.cfg causes the mobile port to block automatically when this error occurs three times in a row:

```
ASRBlock=On
```

When ASRBlock=Off is used, the port will be restarted and will remain open.

The following parameter in the pabx.cfg file allows you to change the default value (30% for 40 calls): GSM=ASR[<percent>,<number of calls>]

```
GSM=ASR[20,35]
```

7.15 RECHARGING PREPAID SIMS

Prepaid SIM cards are an alternative to mobile telephone SIMs with a contract. Instead of being billed retroactively, prepaid SIMs are paid for in advance and then recharged when they run out.

The advantages of prepaid SIMs are:

- No monthly basic fee
- Cost control
- No surprises resulting from unexpectedly high mobile telephone bills

When the account is empty, it can be recharged. The recharging methods for prepaid SIM cards of different carriers vary:

- Recharging via SMS/USSD
- Recharging via call to a defined number
- Recharging via DTMF
- Automatic recharging via direct debit

When prepaid SIMs that do not recharge automatically (e.g. through a credit card) are used in a iGATE, it is possible to recharge them directly from the system. The following requirements apply:

- The SIM is registered and no connection is active.
- Exact knowledge of the mobile carrier-specific recharging procedure exists.
- One valid prepaid voucher exists for one recharge.

Transmission errors, truncated connections, incorrect or altered recharging procedures can prevent successful recharging. Please bear in mind that 3 incorrect recharge attempts (per SIM) can result in blocked SIMs. Recharge SIMs at your own risk. TELES is not liable for any possible loss.

iGATEs support of the following procedures:

- USSD message to the mobile carrier's account manager
  The GATE Manager sends the configured USSD message through the iGATE to the account manager. USSD recharging is the recommended and most reliable procedure, as it consists of a digital message. Unfortunately, only a few mobile carriers currently support USSD recharging. Please ask your mobile carrier if he supports USSD recharging.
- SMS message to the mobile carrier's account manager
  The GATE Manager sends the configured SMS containing the voucher number through the iGATE to the

account manager. Unfortunately, only a few mobile carriers currently support SMS recharging. Please ask your mobile carrier if he supports SMS recharging.

- Connection setup to the account manager with subsequent menu selection and DTMF-tone transmission of the voucher number
  - Direct recharging: Connection setup from a telephone through the iGATE to the account manager and manual DTMF-tone transmission.
  - Indirect recharging using the GATE Manager: The GATE Manager sets up a connections through the iGATE to the account manager and sends the configured DTMF tones automatically.

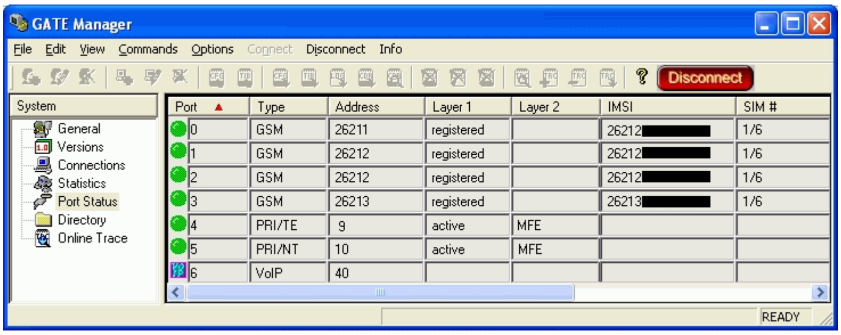
Direct recharging is the simplest procedure. Since a direct connection exists, it is possible to react to commands and error messages immediately. Indirect recharging by means of USSD is the most reliable and quickest way to recharge SIMs if the configuration in the TELES.GATE Manager and iGATE is correct.

7.15.1 RECHARGE PREPARATION

7.15.1.1 CHECKING THE ACTIVE SIM

To avoid recharging the wrong SIM card, be sure to check the mobile controller's active SIM using the GATE Manager:

GATE Manager



Port	Type	Address	Layer 1	Layer 2	IMSI	SIM #
0	GSM	26211	registered		26212[redacted]	1/6
1	GSM	26212	registered		26212[redacted]	1/6
2	GSM	26212	registered		26212[redacted]	1/6
3	GSM	26213	registered		26213[redacted]	1/6
4	PRI/TE	9	active	MFE		
5	PRI/NT	10	active	MFE		
6	VoIP	40				

Figure 7.1 GATE Manager Port Status

Connect to the system and go to the **Port Status** window. The active position in the SIM-card carrier is displayed in the **SIM #** column. The mobile controller's active SIM is displayed in the **IMSI** column.

7.15.1.2 ADDRESSING SIMS USING PORT- AND CONTROLLER-SPECIFIC ROUTING

SIM recharging for a specific mobile controller requires configuration and activation of port- and controller-specific routing entries in the route.cfg or pabx.cfg configuration file. Usually SIM cards are assigned to a carrier's trunk group and all calls through the carrier's network are evenly divided between the mobile controllers in the group. This would also apply to recharge calls.

The routing entry defined here sets up a connection to the network:

`MapAll<in>=<port>*<ctrl>01:<num>`

When the number <in> is dialed, a connection to <num> is set up through <port>*<ctrl>01: You can now manually enter DTMF tones using a telephone.

To recharge all SIMs in the iGATE, configure the following mapping, whereby 4400 is an example for a number that matches the first controller and 12345 is the number for the account manager:

```
MapAll4400=20*0001:12345
MapAll4401=20*0101:12345
MapAll4402=20*0201:12345
MapAll4403=20*0301:12345
MapAll4404=20*0401:12345
MapAll4405=20*0501:12345
MapAll4406=20*0601:12345
.......
MapAll4431=20*0631:12345
```

7.15.1.3 BLOCKING THE PORT CONTAINING THE RECHARGING SIM

If a call is active on the mobile port containing the SIM to be recharged, the recharging process will not occur. For this reason it is better to block the port before recharging the SIM. In the Connections window, you must check the status No Connection on the mobile port. Block Port does not tear down a connection, it only prevents a new connection from being set up.

Port- and controller-specific routing has a higher priority than the Block Port command. This ensures that normal calls are blocked, but recharge calls can be sent through the defined mobile port.

7.15.2 RECHARGING PROCEDURE

7.15.2.1 DIRECT RECHARGING VIA CALL

This is the easiest method when it is possible to set up a telephone connection to the iGATE system via PSTN or VoIP. This call can be connected with the carrier's account manager over a defined mobile controller. This means the call is set up over the controller's active SIM. Then you simply follow the account manager's recharge instructions. After the SIM has been successfully recharged, it can be used again for a certain amount of time.

The call can be set up using a number of methods. This is also possible if there are not enough available telephone numbers to handle all of the system's available mobile controllers.

- DLA via DTMF
  The user calls a defined number in the system. The called number is connected with the DTMF platform. The digits that are transmitted via DTMF match those in the routing entries. When the connection to the account manager has been established, both legs will be connected (see Chapter 7.15.1.2 ⇨).
- GATE Manager (described in Chapter 7.15.2.2 ⇨ below)

That means no BRI connection is necessary for a telephone that is connected directly to the system!

7.15.2.2 INDIRECT RECHARGING VIA GATE MANAGER

This chapter describes automatic recharging of prepaid SIMs using the GATE Manager. It is not necessary to set up a telephone connection to the iGATE. The GATE Manager can set up its own connection to the carrier's account manager and send the pattern of DTMF tones or a USSD message.

Recharging via Call and Transmission of Preconfigured DTMF Tones

This procedure requires exact knowledge of the when and what information the mobile carrier requests. The corresponding pauses following the connect, for menu selection, between the DTMF tones, for correct repetition of the DTMF tones must be correctly configured in the GATE Manager before the call is set up.

This DTMF-tone pattern can be established by testing the recharging process on a mobile phone or by following the directions in Chapter 2.1 and noting the pauses and transmitted digits.

After a connection has been set up between the iGATE and the GATE Manager, select **Commands | Send Call.** The window must contain either **General**, **Version** or **Directory**.

Send Call opens a dialog to initiate calls or recharge SIMs.

To recharge SIMs, the **1st Number** (e.g. 12345) is the mapping to the prepaid platform through a defined controller (e.g. `MapAll12345=20*0101:12345`).

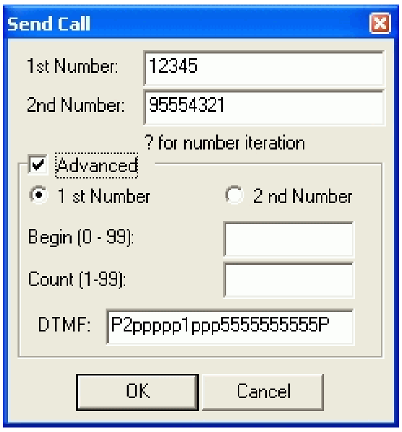
Optional: You can set up a second connection to hear the announcement from the prepaid platform if you enter your own number into the box **2nd Number**. Both connections will be torn down when the second number disconnects. If no number is entered in this box, the call will disconnect when the last DTMF tone has been transmitted or when the last pause interval has passed.

Activate the checkbox **Advanced** to open the **DTMF** box

Enter a series of DTMF tones in the **DTMF** box. Enter a **p** for a pause of 1 second and a **P** for a pause of 10 seconds.

Example: The number for the prepaid platform's account manager is 12345. The telephone number to listen along to the accounting procedure is 5554321, set up through controller 9 (no special routing configuration is defined in the configuration files). Leave this dialog box empty if the accounting process is not to be monitored.
The voucher key is: 55555555555 (a short pause can also be defined between individual digits: for example, 5p5p5p5p5p5p5p5p5p5p5).
To get to the voucher key query, the following pattern must be transmitted: P2ppppp1ppp. Fol-

lowing transmission of the voucher key and a 10-second pause, the call will be torn down.



Send Call

1st Number: 12345

2nd Number: 95554321

? for number iteration

☑ Advanced

● 1 st Number ○ 2 nd Number

Begin (0 - 99):

Count (1-99):

DTMF: P2ppppp1ppp5555555555P

Figure 7.2 Recharging with DTMF Tones

Bear in mind that DTMF tones are only generated with connections into the mobile network. Test calls over the PRI, BRI or VoIP interfaces do not transmit DTMF tones and no tones can be heard!

Recharging via USSD Code (Unstructured Supplementary Services Data)

Recharging prepaid SIMs using the GATE Manager and USSD is the most convenient solution if the prepaid carrier offers this service. The USSD messages contains the prepaid voucher number.

Configure an additional controller in the last position for DTMF functionality as follows:

Example:

```
Controller36=41DTMF
```

The corresponding `Subscriber` line will look like this:

```
Subscriber36=TRANSPARENT ROUTER CHMAX[5]
```

The configuration file route.cfg must contain the following entry in the [System] section:

```
MapAllDTMF=<dtmf port>DTMF
MapAll<place>??=<port>*??01:
```

or

```
MapAll<place>??=<LAIN>*??01:
```

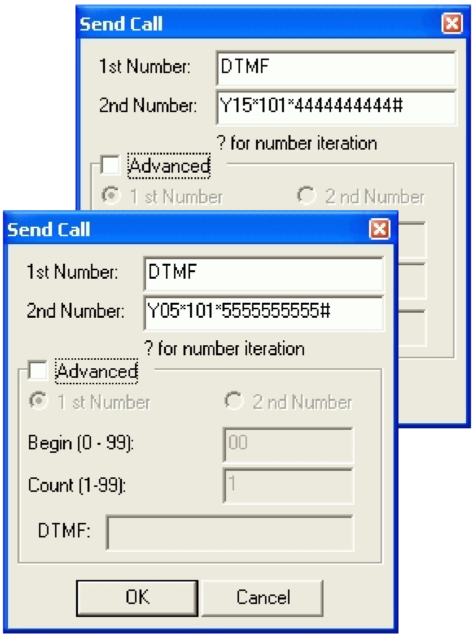
First a placeholder is defined, followed by ?? so that one mapping entry applies for the entire group of the carrier's mobile controllers. The right side of the mapping entry begins with the mobile port number or the port's LAIN.

Example: In the following example, prepaid SIMs from 2 different carriers are used in the system. The letters

Y and Z are used as placeholders, and the carrier's LAINs are 26212 and 26213 (based on the German country code):

```
MapAllDTMF=41DTMF
MapAllY??=26212*??01:
MapAllZ??=26213*??01:
```

Set up a connection to the system through the GATE Manager and select **Commands | Send Call**. Enter DTMF in the **1st Number** dialog box. In the **2nd Number** dialog box, enter the carrier's placeholder (Y or Z) and the number of the controller in which the SIM card is active (15 or 05). Enter a 0 in front of single-digit controller numbers. Then enter the carrier's USSD code (*101*) and the voucher number (44444444444 or 55555555555). The USSD command ends with #.



Send Call

1st Number: DTMF

2nd Number: Y15*101*4444444444#

Send Call

1st Number: DTMF

2nd Number: Y05*101*5555555555#

Begin (0 - 99): 00

Count (1-99): 1

DTMF:

Figure 7.3 Recharging with USSD Codes

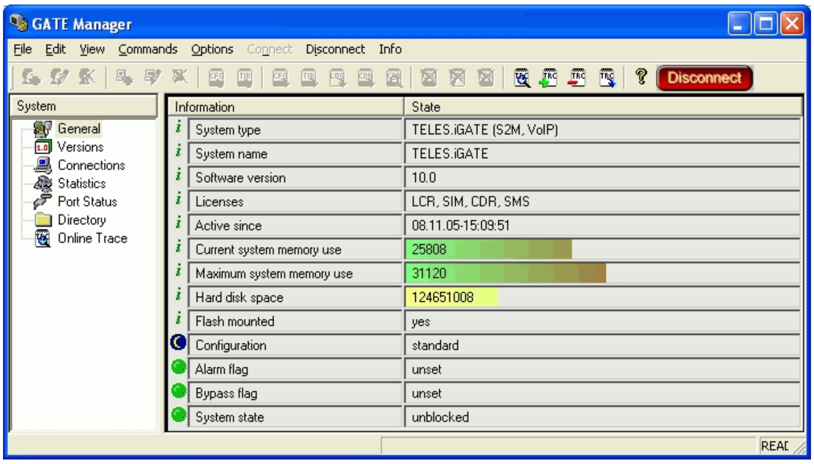
Incorrect USSD commands can result in blocked SIMs or failure in the mobile module!

Configuration entries for recharging confirmation are described in Chapter 3.

Recharging via SMS (Short Message Service)

First of all, please check whether you have the license to send SMS messages on your system.

You will find it in the **General** view under **Licenses** when you connect to the system via GATE Manager.



Information	State
System type	TELES.iGATE (S2M, VoIP)
System name	TELES.iGATE
Software version	10.0
Licenses	LCR, SIM, CDR, SMS
Active since	08.11.05-15:09:51
Current system memory use	25808
Maximum system memory use	31120
Hard disk space	124651008
Flash mounted	yes
Configuration	standard
Alarm flag	unset
Bypass flag	unset
System state	unblocked

Figure 7.4 GATE Manager General View

The name for the license is SMS. This entry is required to send SMS.

You must configure the mail service in the [Mail] section of the file pabx.cfg if you want to send the SMS messages with an e-mail client through a mail server or directly to the iGATE:

```
[Mail]
SmtpServer=<server addr>
```

MailRcpt=<domain>

MailFrom=<own address or name>

This entry is not necessary when using only the GateManager's Send SMS command.

The third entry in the mobile controller's `Subscriber` line is the SMS center number:

```
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+00000,1,1,1,SIMS,IMSI] CHADDR ALARM
```

German example:

```
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,+491721111,1,1,1,SIMS,IMSI] CHADDR ALARM
```

You must restart the system to activate the changes.

Then enter the port-specific SMS settings:

```
MapAllSMS<shortnumber>=LAIN*0001:<number>
MapAllSMS<shortnumber>=port*0001:<number>
```

Example: In the following German example with LAIN numbers, the short number 00 is routed to the first controller. The number 12345 is sent to the SMS center.

```
MapAllSMS00=26212*0001:12345
MapAllSMS01=26212*0101:12345
MapAllSMS02=26212*0201:12345
MapAllSMS03=26212*0301:12345
MapAllSMS04=26212*0401:12345
MapAllSMS05=26212*0501:12345
MapAllSMS06=26212*0601:12345
……
```

If the SMS is sent with a normal e-mail client, the keyword **SMS** will appear in the **To** dialog box, followed by the short number, which indicates the mobile controller. An **@** sign and the iGATE's IP address or name if the system is attached to a DNS server will follow. The message box contains the recharge code in the carrier's syntax.

```
SMS00@<ipaddr>
SMS00@<domain>
```

If the SMS is used with the Send SMS command in the GATE Manager's **Commands** menu, use only the short number and not the keyword SMS.

To save the recharge platform's confirmation e-mail, the e-mail can be sent to an account using the following entry in the route.cfg:

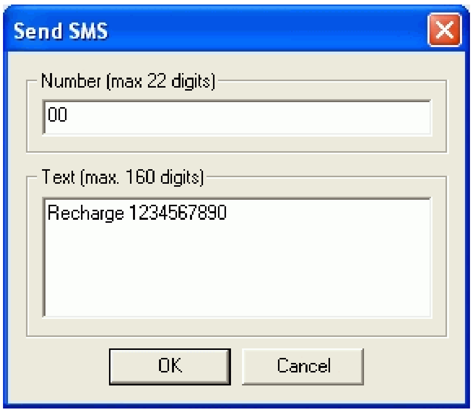
```
Restrict<port>=@<addressee> 05
```

It can also be saved into a file using the following entry in the pabx.cfg:

```
MsgLog=/data/msg.log
```

To save it into a file, the following entry in the route.cfg is also required:

```
Restrict<port>=@FILE 05
```



Send SMS

Number (max 22 digits): 00

Text (max. 160 digits): Recharge 1234567890

Figure 7.5 Send SMS

Example: In the following example for saving the SMS into a file, all incoming SMS to LAIN 26212 is saved into the file msg.log:

```
Restrict26212=@FILE 05
```

If the e-mail is sent to an account, the routing entry will look like this:

```
Restrict26212=@nase 05
```

Use the following entries in the `pabx.cfg` to connect the iGATE to an e-mail server:

```
[Mail]
SmtpServer=<server address>
MailRcpt=<domain>
MailFrom=<own address or name>
```

7.15.3 PREPAID ACCOUNT STATUS QUERY

After a SIM card has successfully been recharged, you can query its current account status. The following variations are possible:

- Direct query via call
- Indirect query with the GATE Manager
- Listening in on the GATE Manager connection
- USSD account-status query

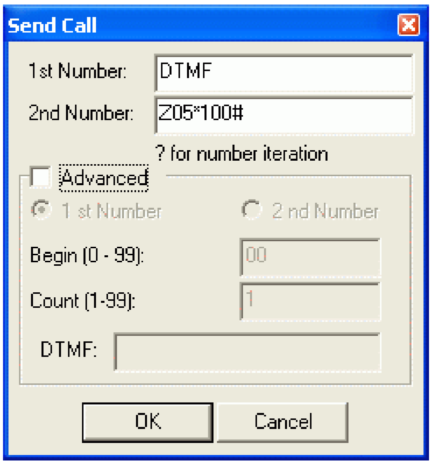
7.15.3.1 DIRECT ACCOUNT-STATUS QUERY

The same basic settings apply here as have already been described for SIM recharging.

That means routing configurations must be entered that set up a connection between the caller and the carrier's prepaid platform. Use the same routing configuration described in Chapter 7.15.2 ⇨. The only difference is that you will select the account-status query instead of account recharging from the menu.

7.15.3.2 INDIRECT ACCOUNT-STATUS QUERY

The indirect method with the GATE Manager and listening in on the connection requires a change in the pattern of DTMF tones. You must, of course, know what the pattern is beforehand, and then you must configure it in the **Send Call** dialog.



Send Call

1st Number: DTMF

2nd Number: Z05*100#

? for number iteration

□ Advanced

● 1 st Number ○ 2 nd Number

Begin (0 - 99): 00

Count (1-99): 1

DTMF:

Figure 7.6 Status Query

The indirect USSD account-status query corresponds with the USSD recharging procedure with altered USSD account-status-query command instead of the recharging command with cash code (voucher number).

The USSD recharging procedure results in an immediate USSD response message, so that the iGATE does not require an explicit query following USSD recharging.

7.15.3.3 SAVING /FORWARDING THE ACCOUNT STATUS

Account-status information can be saved to a file in the iGATE. The following entry in the pabx.cfg is required:

```
MsgLog=/data/msg.log
```

The corresponding routing entries in the route.cfg configuration file will look like this:

```
Restrict<port>=@FILE 06
Restrict<LAIN>=@FILE 06
```

Example: The following example shows incoming USSD messages for 2 carriers:

```
Restrict26212=@FILE 06
Restrict26213=@FILE 06
```

The USSD entry in the file will appear in 2 lines as follows:

```
Date Time [Port] IMSI
USSD Message Text
```

Example:

```
14.02.05-17:40:06 [04] 262125555555555
Current Cash Account: 143,83 Euros
```

7.16 DEFINING SPECIAL CHARACTERS FOR VOICE CALLS

In cases in which the called number includes special characters (e.g. * or #), it may be necessary to define the call type used in the mobile network (command or voice call). Calls to GSM or CDMA that begin with * or #, are sent as command calls by default. For voice calls beginning with * or #, you must define the call type voice in the mapping entry with a > sign.

The routing entry will look like this:

```
MapAll<num>=<LAIN>><num>
```

Example:

```
MapAll222=11111>*222
```

8 SIGNALING AND ROUTING FEATURES

8.1 DIGIT COLLECTION (ENBLOCK/OVERLAP RECEIVING)

This function makes it possible to collect digits and transmit calls when a specific number of digits has been dialed. The entire call number is required for the call to be set up with a mobile phone or the mobile gateway. Since most numbers have a uniform number of digits, the mobile gateway can collect digits when calls enter the gateway in overlap mode. Digit collection occurs through the following mapping command:

```
MapAll<direct>=|<num><<<digits>
```

The **|** (pipe) signifies that the following digits will be collected before they are transmitted, and <digits> is the total number of the port digits and the digits of the called party number. This figure can range between 00 and 24 and must be entered in double digits. The parameter `DTMFWaitDial` defines the number of seconds the system waits between the individual digits (default 5). Please bear in mind that you can configure a maximum of 11 digits in the first part of the command and 19 (including a special character, e.g. #) in the second. The call will be forwarded as soon as the specified number of digits has been dialed or a time-out limit has been reached.

Example: The following example shows a call with the prefix 01555. The **|** (pipe) signifies that the following digits will be collected before they are transmitted. The 14 at the end is the sum of the port digits and the digits of the called party number (e.g. |#20=3, 01555899666=11, 3+11=14).

```
...
MapAll01555=|#2001555<<14
...
DTMFWaitDial=5
...
```

8.2 REJECTING DATA CALLS AND SPECIFIED NUMBERS

This chapter describes the configuration options for exclusion of data calls, prefixes, or call numbers from the routing process.

8.2.1 BLACKLIST ROUTING

The system will reject all calls directly if the MapAll entry contains the keyword & followed by the two-digit cause value (see ETS 300 102-1).

```
MapAll<direct>=&<cause>
```

A maximum of 5000 MapAll entries per time zone can be defined. For more than 5000 entries, please use the iMNP.

Example: In the following example, all calls to the number 004915551234 and all service calls with the prefix 0180 are rejected with a busy signal. All other calls are sent to the VoIP profile DF:

```
MapAll015551234=&91
MapAll004915551234=&91
MapAll0180=&91
MapAll0=40DF:0
...
MapAll9=40DF:9
```

8.2.2 WHITELIST ROUTING

The following entries enable exclusion of specific OADs or trunk groups:

```
Restrict<ns>=<pl>
MapAll<pl>=&<cause>
```

NS refers to the internal controller number and the call's origination address.

A maximum of 1000 Restrict entries per time zone can be defined.

Example: In the following example, the numbers 12345 and 12346 connected to the PBX at port 10 cannot make any international calls. All national calls are sent to the VoIP profile DF and all local calls are sent to the PSTN:

```
Restrict1012346=int
MapAllint00=&91
MapAllint0=40DF:0
MapAllint1=91
...
MapAllint9=90
```

Example: In the following example, all incoming calls from the mobile port trunk groups 26212 and 26213 are rejected with a busy signal:

```
Restrict26212=not
Restrict26213=not
MapAllnot=&91
```

8.2.3 REJECTING CALLS WITH ISDN BEARER CAPABILITY DATA

ISDN data calls can be handled differently from voice calls depending on the configuration of the call types DATA or VOICE. This setting is especially interesting for VoIP or GSM calls:

```
MapAll<direct>=&<cause> <mode>
```

Analog modm connections are not included in this configuration, as they generally do not have a specified bearer capability.

Example: In the following example, all ISDN data calls are rejected with the cause value AA (switching equipment congestion). All calls with the prefix 0170 are routed to the mobile trunk group 26211 and all other calls are routed through VoIP:

```
MapAll0=&aa DATA
...
MapAll9=&aa DATA
...
MapAll0170=262110170
MapAll0=40DF:0
...
MapAll9=40DF:9
```

8.2.4 SPECIFIC ROUTING OF DATA CALLS VIA VOIP

In the ISDN network, data calls have a special service type. When an ISDN PBX is connected to a VoIP network, it must continue to work without any problems (e.g. PBX remote maintenance calls or ISDN terminal adapter). In the case of VoIP, a specific RTP payload type is used: trp, ccd or gnx64.

Example: In the following example, two VoIP profiles are configured, so that all calls are routed, regardless of whether they are data calls or voice over IP calls. The first one is for outgoing voice calls and all calls from VoIP to ISDN. The second profile is exclusively for outgoing data calls, so that signaling consists solely of clear mode in SDP:

```
MapAll0=40DATA:0 DATA
...
MapAll9=40DATA:9 DATA
MapAll0=|40DF:0<<24
...
MapAll9=|40DF:9<<24
Restrict40=In
MapAllIn=10
[Voip:DF]
VoipDirection=IO
...
VoipCompression=g711a g729 trp t38
...
[Voip:DATA]
VoipDirection=Out
...
VoipCompression=trp
VoipECE=No
...
```

8.3 CLIP AND CLIR

8.3.1 ROUTING CLIP AND CLIR CALLS

This function allows you to route calls with Calling Line Identification Presentation (CLIP) differently from calls with Calling Line Identification Restriction (CLIR). For example, all CLIP calls can be rejected, so that only calls that do not present the calling number or calls without a calling party number (e.g. analog) are transmitted through the iGATE.

Use the following configuration to define the various routing methods:

```
...
InsertCLIR=On
...
Restrict9=OK 01
Restrict|9=OK 01
Restrict90=FAIL 01
...
MapInOK00491555=2200491555
MapInFAIL=&aa
...
```

InsertCLIR=On activates this mode. 01 is the service indicator for telephony (analog and ISDN) and is used to differentiate these calls from remote administration calls. Restrict9=OK 01 means that all telephony calls without a calling number are put through. Restrict|9=OK 01 means that all CLIR telephony calls are put through. Restrict90=FAIL 01 means that all CLIP telephony calls are rejected with No Channel Available as rejection cause when they are mapped to MapInFAIL=&aa.

8.4 ROUTING CALLS WITHOUT CLIR

This function enables you to bypass CLIR for calls through the defined mobile port. The following configuration in `pabx.cfg` activates this function:

```
Subscriber<xx>=...GSM[...,!CLIR]...
```

When this function is configured, the SIM's telephone number (and not originating telephone) is always transmitted to the B subscriber.

8.4.1 SETTING CLIR

Setting a hash (#) in front of a call number makes it possible to suppress the presentation of the origination number of calls regardless of how the call comes into the system.

The following sytax is used: `MapAll<num>=#<port><num>`

Example: The following example shows an appropriate configuration. With this entry, all calls beginning with 00491555 are sent to the port with the address 22 and the presentation of the number is restricted:

```
MapAll00491555=#2200491555
```

8.4.2 SETTING CLIP

Setting an exclamation point (!) in front of a call number makes it possible to force the presentation of the origination number of calls regardless of how the call comes into the system.

The following sytax is used: `MapAll<num>=!<port><num>`

Example: The following example shows an appropriate configuration. With this entry, all calls beginning with 004930 are sent to the port with the address 9 and the presentation of the origination number is allowed.:

```
MapAll004930=!9004930
```

8.5 CONVERSION OF CALL NUMBERS

The conversion of call numbers makes it possible, for example, to implement number portability or to redirect calls when the user can be reached at another number. In the following mapping command, the call number 015550123456 is changed to 015559876543 and sent to the mobile channel (MapAll...=20..):

Example 1

```
...
MapAll015550123456=20015559876543
```

Example 2 ⇨ presents an alternative, in which the routing file is searched through again after conversion of the call number to determine the route for the prefix `01555`. Please bear in mind that you can configure a maximum of 1499 mapping entries with no more than 11 digits in the first part of the command and 19 in the second.

Example 2

```
...
MapAll015550123451=$Reception
MapAll015550123452=$Reception
MapAll015550123453=$Reception
MapAllReception=015559876543
```

8.6 SETTING NUMBER TYPE IN OAD/DAD

In some cases it may be necessary to set a specific number type for the OAD or DAD. There are different methods for the various interfaces. The following number types can be set:

Table 8.1 Number Types

Type	Definition
u	Unknown
s	Subscriber number
n	National number
i	International number

OAD

Use the following entry to set a specific number type in the OAD:

```
Restrict<port><num>=<type> 15
```

For the national and international types, remove the 0(s) at the beginning of the number:

```
Restrict<port>0=n 15
Restrict<port>00=i 15
```

Example: In the following example, the bit is set in the caller's origination number for a call via BRI controller 01:

```
Restrict90=n 15
Restrict900=i 15
```

Example:

You can set a u (unknown type of number) in the Restrict entry to change transmission of the national/international bit to 0 or 00 at the beginning of the OAD. As in a mapping entry, the national/international bit will always appear left of the equal sign as 0 or 00.

```
Restrict<port>0=u0 15
Restrict<port>00=u00 15
```

In the following example, the area code 030 with a 0 at the beginning of the OAD of the PBX's extension is set as a digit and transmitted along with the number:

```
Restrict10555=u030555 15
```

`Restrict` entries are handled from general to specific from top to bottom.

DAD

Enter one of the four specific number types in the DAD as follows:

```
MapAll<num>=<port><type><num>
```

In the case of a VoIP controller, enter the following:

```
MapAll<num>=<port><voip profile>:<type><num>
```

The number type will then be defined at the port. For the national and international types, remove the 0(s) at the beginning of the number:

Example: In the following example, the international bit is set for all calls to Italy (0039) and the number is transmitted with 39. For the area code 012, the national bit is set and the number is transmitted with 12:

```
MapAll0039=40iG1:i39 VOICE
MapAll012=40iG1:n12 VOICE
```

General Example

Example: In the following example, a 1:1 routing entry for the individual PRI controllers to VoIP appears in addition to the international flag from PRI to VoIP. A placeholder routing entry is used (bla or blu), in which the PRI ports are directly assigned to a mapping. Traffic at PRI port 9 is sent directly to VoIP port 40 with the VoIP profile iG1. Traffic from PRI port 10 is sent to VoIP port 40 with the profile iG2:

```
Restrict9=bla
Restrict900=i 15
Restrict10=blu
Restrict1000=i 15

MapAllbla00=40iG1:i
MapAllblu00=40iG2:i
```

The `restrict` entries for the individual ports must appear in the following order: placeholder, OAD international flag, DAD routing with international flag.

8.7 SETTING THE SCREENING INDICATOR

You can set the screening indicator to define whether the calling-party number sent is specified as user provided verified and passed or network provided:

User provided verified and passed: v

Example: In the following Restrict example, the calling party number sent is specified as user provided verified and passed:

```
Restrict10=v 15
```

Network provided: p

Example: In the following Restrict example, the calling party number sent is specified as network provided:

```
Restrict10=p 15
```

If you also want to define a number type (see Chapter 8.6 ⇨), it must appear in front of the screening indicator:

Example: In the following Restrict example, the screening indicator is specified as network provided, and the number type is international:

```
Restrict10=ip 15
```

Example: Please bear in mind that this entry will not work if you set a minus sign (-) behind VoipOad=<num>.

8.8 SETTING A DEFAULT OAD

Use the Restrict command to set a default origination number (*<oad> 15) when the OAD is restricted (<num>):

`Restrict<port><oad>=*<num> 15`

Example: In the following example, 12345 replaces the original OAD. When the destination number begins with 030, the call is sent through controller 10:

```
Restrict9=*12345 15
MapAll030=10030
```

Use the entry Restrict<port><oad>=<num> 15 if digits at the beginning of the OAD are the only ones to be restricted.

Example: In the following example, the digits 004930 are replaced with 030 followed by the remaining digits. The destination number begins with 030 and is sent through port 10.

```
Restrict9004930=030 15
MapAll030=10030
```

8.9 SETTING OR REMOVING SENDING COMPLETE BYTE IN SETUP

In some cases the ISDN or H323 peer system may require this byte for routing, or the byte may disrupt signaling.

Setting Sending Complete

The following entry ensures that the Setup includes a Sending Complete:

`MapAll<direct>=)<num>`

The) causes inclusion of Sending Complete in the ISDN Setup or in the H323 Setup.

Example: In the following example, all calls beginning with 0 are sent with a Setup Complete to controller 9:

```
MapAll0=)90
```

Removing Sending Complete

The following entry ensures that the Setup never includes a Sending Complete:

`MapAll<direct>=(<num>`

The (causes removal of Sending Complete in the ISDN Setup or in the H323 Setup.

Example: In the following example, all calls beginning with 0 are sent without a Setup Complete to VoIP controller 40. The VoIP profile is **DF**:

```
MapAll0=(40DF:0
```

8.10 MISCELLANEOUS ROUTING METHODS

In the following scenarios it may occur that some call numbers must be routed with differing lengths or that some call numbers may require additional number conversion:

- Calls without a destination number
- Connection to a PBX with an extension prefix
- Routing based on the length of the destination number

8.10.1 ROUTING CALLS WITHOUT A DESTINATION NUMBER

Enter the following configuration in the route.cfg if the iGATE must route calls that come in without a destination number:

```
Restrict<port>=<pl>
MapAll<pl><num>=<port><num>
MapAll<pl>=<port>
```

Incoming calls from the configured port will be assigned a placeholder and then all calls beginning with the placeholder will be routed to the placeholder's placeholder's mapping.

Example: In the following example, all calls from controller 9 are routed to controller 10, regardless of whether a destination number appears in the setup:

```
Restrict9=pl
MapAllpl=10
```

8.10.2 ROUTING CALLS BASED ON AN EXTENSION PREFIX OR ON THE LENGTH OF THE DESTINATION NUMBER

To route calls with a DAD differently from those without a DAD, you must activate the block feature in the pabx.cfg and restart the system:

```
Block=1
```

Set all other parameters in the route.cfg. First define the port from which the incoming calls are to be routed. Incoming calls from the configured port will be assigned a placeholder and then digit collection will occur for all calls beginning with the placeholder. The $ in the mapping entry, followed by the defined placeholder (MMM), causes a second search of the routing file when the number is complete:

```
DTMFWaitDial=<sec>
Restrict<port>=<pl>
MapAll<pl>=|$MMM<<98
```

The second routing-file search is based on the routing entry with the leading placeholder (MMM):

```
MapAllMMM<digits>=<dest><digits>
```

Example: In the following example, digit collection is activated for all calls that come into port 9. Calls with the destination number 2222 are sent to the VoIP controller with the profile DF and the destination number is replaced with the SIP account Betty. Calls with the num-ber 3333 are sent to VoIP with the SIP account Al. All other calls with a destination number are sent to controller 10. Calls without a destination number are sent to the number 12345 at port 10:

```
DTMFWaitDial=5
Restrict9=pl
MapAllpl=|$MMM<<98
MapAllMMM2222=40DF:Betty
MapAllMMM3333=40DF:Al
MapAllMMM0=100
MapAllMMM1=101
MapAllMMM2=102
MapAllMMM3=103
MapAllMMM4=104
MapAllMMM5=105
MapAllMMM6=106
MapAllMMM7=107
MapAllMMM8=108
MapAllMMM9=109
MapAllMMM=1012345
```

8.11 CHANGING CAUSE VALUES

It is possible to group cause values together into a single defined cause value so that rejected calls can be handled in a specified manner by the switch sending the call to the iGATE. The following cause value groups can be defined in the pabx.cfg:

Group 0 Cause Values

All connections that are rejected with a group 0 cause value (0x80-0x8f) can be mapped to a single cause value by entering TranslateG0Cause=<cau>, whereby <cau> represents a cause value in hexadecimal form.

Group 1 Cause Values

All connections that are rejected with a group 1 cause value (0x90-0x9f) can be mapped to a single cause value by entering TranslateG1Cause=<cau>, whereby <cau> represents a cause value in hexadecimal form.

Group 2 Cause Values

All connections that are rejected with a group 2 cause value (0xa0-0xaf) can be mapped to a single cause value by entering TranslateG2Cause=<cau>, whereby <cau> represents a cause value in hexadecimal form.

Group 3 Cause Values

All connections that are rejected with a group 3 cause value (0xb0-0xbf) can be mapped to a single cause value by entering TranslateG3Cause=<cau>, whereby <cau> represents a cause value in hexadecimal form.

Translating Individual Cause Values

The following parameter allows you to translate any of these cause values to any other one: Translate<cause>=<cause>. The values entered must be in hexadecimal notation between 00 and 7f.

Translating SIP Causes to ISDN and Vice Versa

You can define a specific translation from SIP responses (4xx - 6xx) to ISDN cause values and vice versa. If nothing is set, the translation occurs as described in `draft-kotar-sipping-dss1-sip-iw-01.txt`

Use the following parameter to translate a cause from ISDN to a specific SIP response:

```
SipCause<ISDN cause>=<SIP Response>
```

Repeat the entry to initiate an additional translation.

Use the following paramter to translate a cause from SIP to ISDN:

```
SipEvent<SIP Response>=<ISDN Cause>
```

The following range of values applies:

400<= <SIP Cause> <=699	(defined in RFC 3261)
0<= <ISDN Cause> <=127	(DSS1 decimal cause number)

9 ADDITIONAL VOIP PARAMETERS

You can enter the following additional parameters in the route.cfg to adjust the configuration for improved communication with the VoIP peer.

9.1 SIGNALING PARAMETERS

Table 9.1 Customized Parameters: Protocol-Independent VoIP Signaling

Protocol-Independent VoIP Signaling Parameters
VoipDad=<num> The digits/numbers defined here will appear in front of the original DAD. If the parameter is to be valid in only one direction, you must set another profile without this parameter for the other direction.
VoipOad=<num> The digits/numbers defined here will be transmitted in front of the original OAD. If a minus (-) is entered, the original OAD will not appear. Only the digits entered in front of the minus sign will be displayed. If the parameter is to be valid in only one direction, you must set another profile without this parameter for the other direction. To limit this feature to OADs consisting of a certain number of digits, enter a !, followed by the number of digits, at the end of the entry. In the following example, the digits 567 will appear only if the OAD has at least 6 digits: EXAMPLE: `VoipOad=567!6` To modify the original OAD, enter `randomx`, whereby x represents a number of random digits that will appear in the OAD. EXAMPLE: `VoipOad=567random2-`
VoipProgress=<int> For H.323: 0=progress indicator is not transmitted. 1 (default)=progress indicator is transmitted. 2=address complete message is transmitted. 3=call proceeding message type changed in alerting message type. For SIP: 0=183 response ignored and not sent. 1=183 response changed to a progress message with inband-info-available at the ISDN interface (default). 2=183 response changed to an address complete message at the ISDN interface. 3=183 response changed to an alerting at the ISDN interface.
VoipComprMaster=<mode> This parameter defines which side the first matching codec comes from: `Yes`: Default. Priority is determined by the order of the system's parameter list. `No`: Priority is determined by the peer.

Table 9.1 Customized Parameters: Protocol-Independent VoIP Signaling *(continued)*

Protocol-Independent VoIP Signaling Parameters
VoipHideOadByRemove=<mode> If Yes is configured and call setup is to VoIP, the OAD will be removed from signaling if presentation restricted or user-provided, not screened is set in the calling party's presentation or screening indicator. No (default) means no change will occur. **NOTE: If the SIP protocol is used, Anonymous will always appear as the account in the From field. Transmission of the OAD can occur in the P-asserted header.**
VoipSignalCLIR=<string> When the configured string appears at the beginning of the OAD and the parameter VoipHideOadByRemove is set, the OAD is removed from signaling, regardless of the presentation bits in the calling party field. If the parameter VoipHideOadByRemove is not set (default), the presentation bits are set at presentation restricted (CLIR) if <string> is -. If the string matches the first digits of the OAD and it comes in with CLIP, the call will be sent to VoIP using CLIR. If the call comes in with CLIR, the string will be added to the beginning of the OAD and CLIR will be removed in the signaling.
VoipSingleTcpSession=<mode> Enter Yes to send all outgoing VoIP connections in a single TCP session. Enter No (default) for an extra TCP session for each VoIP connection.
VoipIgnoreDADType=<mode> Enter yes to change the DAD type to unknown, e.g. from international. The type is lost, e.g. the leading 00 bit is removed. Default no.
VoipSuppressInbandInfoAvailableIndicatorInCallProceeding=<mode> Enter yes to send or receive the Progress Indicator in the Q.931 Call Proceeding message. Default no.
VoipG72616PayloadType=<num> Changes the SIP payload type for G.726 16 b/s. Default is 35. A common value is 102.
VoipG72624PayloadType=<num> Changes the SIP payload type for G.726 24 b/s. Default is 36. A common value is 99.
VoipTrpPayloadType=<num> Defines the payload type for data calls when trp (transparent/clear mode) is used as codec in VoipCompression=<list>. Default is 56. A common value is 102.
VoipDataBypassPayloadType=<num> Defines the payload type for the RTP packets when the call is sent as a data call. Default 96.

Table 9.2 Customized Parameters: H.323 Signaling

H.323 Signaling Parameters
VoipService=0x<service indicator> This parameter sets the barrier capability. For example, it can be used for calls coming from VoIP with the barrier capability data. You can define the service indicator as it is in the 1TR6 code: 101 - ISDN 3,1kHz 102 - analog 103 - ISDN 7kHz 201 - Fax 2 202 - Fax 3 203 - Fax 4 700 - Data Normally 101 is used. You can send another value to a switch that wants to handle VoIP calls differently from PSTN calls. EXAMPLE: `VoipService=0x101`
VoipMapAddressType=<mode> For calls from PSTN to VoIP only. Enter `yes` to change the 00 at the beginning of a number to international and 0 to national.
VoipSetupAck=<int> 1=setup acknowledge is transmitted; 0= setup acknowledge is not transmitted; 2 (default) =transmitted with H.323 information.
VoipH245Transport=<int> This option determines the H.245 offer. 0 (default)=all signaling variants are offered; 1=FastStart only; 2=H.245 tunneling only; 3=extra session.
VoipCanOverlapSend=<mode> Enter off to deactivate overlap sending during setup (default on).
VoipRestrictTCS=<mode> If Yes is entered, the response in the H.323 tunneling terminal capability set contains only the codecs offered by the peer and not those configured in the system. Default No.

Table 9.3 Customized Parameters: SIP Signaling

SIP Signaling Parameters
VoipOwnAddress=<account@domain> Used for the `From` field in Sip-Invite and Sip-Response messages. If only the domain is entered, the origination address (e.g. from ISDN) followed by an @ sign will automatically be set at the beginning.
VoipOwnDisplay=<string> The entry is sent as Display Name in the `From` Field in SIP transmissions. The keyword `MSN` causes the calling telephone's MSN to be transmitted as Display Name. Example: From: "John" <sip:493011111@teles.de>
VoipContact=<account@domain> Used for the `Contact` field in Sip-Invite and Sip-Response messages.
VoipP-Preferred-Identity=<string> Sets the P-Preferred-Identity field in the SIP invite message. The following settings are possible toward SIP: `*` The OAD coming from ISDN is transmitted. `<string>` The defined string is transmitted A combination of both is possible. Examples: 030* or tel:* or sip:user@carrier.de
VoipP-Asserted-Identity=<string> Sets the P-Asserted-Identity field in the SIP invite message. The following settings are possible toward SIP: `*` The OAD coming from ISDN is transmitted. `<string>` The defined string is transmitted A combination of both is possible. Examples: 030* or tel:* or sip:user@carrier.de
VoipOadSource=<int> SIP only: defines the field from which field the calling party number coming from SIP is to be taken: 0 = From: field (default) 1 = Remote-Party-ID 2 = P-Preferred-Identity 4 = P-Asserted-Identity **NOTE: If 2 or 4 are entered, the number in the field must begin with tel:** Going to SIP, the OAD is written in the following field: 0 = From: field (default) 1 = Remote-Party-ID (if VoipOwnAddress is not set) for the fields P-Preferred-Identity and P-Asserted-Identity, please check the corresponding parameters.

Table 9.3 Customized Parameters: SIP Signaling *(continued)*

SIP Signaling Parameters
VoipDadSource=<int> SIP only: defines the field from which field the called party number coming from SIP is to be taken: 0 = URL 1 = To: field 2 = Remote-Party-ID with party = called
VoipUseMaxPTime=<mode> SIP only. Enter yes to set the field mptime (max packet time) with the values set in VoipTxm (ptime). Default no. The parameter VoipUseMaxPTime is used when VoipUseMPTime is 0, 1 or 2.
VoipUseMPTime=<int> This parameter is used to configure packet time signaling in SDP: 0 = set attribute ptime with each individual codec description (default). 1 = set attribute ptime once as the first attribute after the m- line (media type). 2 = set attribute mptime (multiple ptime) once as the first attribute with the list of the codecs' corresponding ptimes. 3 = remove attribute ptime or mptime in SDP signaling. The parameter VoipUseMaxPTime is used when VoipUseMPTime is 0, 1 or 2.
VoipPrack=<mode> SIP only: Enter yes to activate Provisional Response Messages in the signaling, as per RFC 3262 "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)". Default is no.
VoipOverlap=<mode> SIP only. Enter `yes` to activate signaling with overlap sending, as per draft-zhang-sipping-overlap-01.txt. That means digit collection is no longer necessary in the routing when the digets come from ISDN with overlap sending. When this parameter is active, VoipPrack is automatically set to yes. Default is no.

Table 9.3 Customized Parameters: SIP Signaling *(continued)*

SIP Signaling Parameters
VoipSdpProxy=<mode> SIP only. Enter `yes` to activate proxy mode for SDP signaling for SIP to SIP calls. The parameters for RTP signaling will be forwarded from one leg to the next and RTP is not handled by the system. Default is no.
VoipInfoSamOnly=<mode> This parameter determines the behavior in the case of overlap sending (VoipOverlap must also be set). Yes means that the contents of the SubsequentNumber field in info method will be attached to the URI's available digits or to the invite message's To field. No (default) means that the digit contents of the SubsequentNumber field will be used.
VoipAllow=<list> The allow header shows the supported methods and can be set here. EXAMPLE: VoipAllow=INVITE,BYE The default setting includes the following: INVITE,ACK,CANCEL,BYE,UPDATE,REGISTER,PRACK,INFO,NOTIFY,REFER It may be necessary to remove some of these entries for some peers.
VoipDelayDisc=<mode> Yes (default) delays confirmation transmission during call teardown. That means the release tone is audible when the peer tears down the call. **NOTE: For versions 13.0c or lower: To improve ASR, we recommend that you set this parameter to `Yes` if you use the parameter `VoipMaxChan`.**

9.2 REGISTRAR PARAMETERS

The following parameters can be used in the VoIP profile when the SIP agent wants to register with the iGATE.

Table 9.4 Customized Parameters: Location Server

Location Server Parameters
VoipOwnUser=<string> Defines the username the agent uses to register.
VoipOwnPwd=<string> Defines the password the agent uses to register.
VoipExpires=<sec> Defines the maximum number of seconds the agent's registration applies (default 3600).
VoipAuth=<mode> Defines the authentication procedure `www` (default) or `proxy`.

Example: The following example creates an account for a user agent with the username 130 and password test130. Authentication occurs with the procedure www:

```
MapAll130=40U1:130

[Voip:U1]
VoipDirection=IO
VoipIpMask=0x00000000
VoipOwnUser=130
VoipOwnPwd=test130
VoipExpires=300
VoipAuth=www
VoipCompression=g711a g711u g729 g729a g729b g729ab
VoipSilenceSuppression=no
VoipSignalling=1
VoipMaxChan=8
VoipTxM=2
VoipDtmfTransport=0
VoipRFC2833PayloadType=101
VoipMediaWaitForConnect=Tone
```

9.3 ROUTING PARAMETERS

Table 9.5 Customized Parameters: VoIP Routing

VoIP Basic Parameters

VoipOadMask=<num>
VoipDadMask=<num>
It is also possible to define the profile by destination or origination number (and not only by the IP address). That means you can use different parameters not only for different IP addresses, but also for different numbers (e.g. other codec, WaitForConnect, etc.). For example, you can define a number for the head of the company, so that her MSN always uses G.711.
It is possible to configure a list of numbers for a total of up to 80 characters per line. You must define the entry again if you need more numbers. You can also use a wildcard * at the end of the number to match all calls with OADs or DADs beginning with the digits entered. Use a coma to separate the numbers. Example:
`VoipDadMask=123, 345*, 567, ....,`
`VoipDadMask=912, 913*, 914, ....,`
`....`
Bear in mind that you must enter numbers from specific to global (as for normal routing in the route.cfg). That means you must enter a profile with more specific numbers above a profile with more global numbers.

VoipUseIpStack=<mode> Enter Yes to facilitate direct use of an xDSL or dial-up connection if the corresponding profile is defined. Default is No.
VoipUseEnum=<mode> Enter yes (default no) to activate an ENUM query to the called number before the call is set up via VoIP or PSTN. Using a standard DNS query, ENUM changes telephone numbers into Internet addresses. If a number is found, the call is set up via VoIP. If not, call setup occurs via PSTN or with another VoIP profile. **NOTE: The query must include country and area codes.**
VoipEnumDomain=<string> Use this parameter to modify the domain name for the enum query (default is `e164.arpa`).
VoipUseStun=<mode> Enter yes (default yes) to use the STUN values for the VoIP profile.
VoIPOwnIpAddress=<ip addr> If the system is behind a NAT firewall that does not translate H.323 or SIP, the NAT firewall's public IP address is transmitted as own IP address in the H.323 or SIP protocol stack (not the private IP address). In this case, the public IP address must be defined. Bear in mind that the NAT firewall transmits the ports for signaling and voice data to the iGATE's private IP address.

9.4 QUALITY PARAMETERS

Table 9.6 Customized Parameters: VoIP Quality

VoIP Quality Parameters
VoipSilenceSuppression=<mode> Activates silence suppression (see Table 5.21 ⇨).
VoipBandwidthRestriction=<mode> Enter Yes to include the VoIP profile in traffic shaping. Default is No. For a description of the functionality, please refer to VoipMaximumBandwidth in Table 5.17 ⇨.
VoipMediaWaitForConnect=<mode> This parameter allows you to influence the system's behavior in relation to voice channel negotiation (RTP stream). The following settings are possible: No (default): RTP data is transmitted immediately after negotiation for RTP. SIP: Early Media is activated; SDP is sent with 183 or 180. Yes: The negotiation of RTP data is sent only after the connection has been established. SIP: SDP is sent only with 200 and ack. Tone: The VoIP peer or the connected PBX requires generation of inband signaling tones (alert, busy, release). **NOTE: If Tone is entered, the tones are not played in the direction of the PBX if RTP is already exchanged before connect (inband is switched through).** Bear in mind that the parameter SWITCH in the VoIP controller's Subscriber line must be removed if the tones are played for the PBX. If Tone is entered and the tones are played to VoIP, the VoIP media channel cannot be released following an ISDN call disconnect as long as the tones are being transmitted. This can result in CDR errors on the peer side.
VoipRtpTos=<num> Enter a value between 0 and 255 to set the TOS (type of service) field in the RTP packet IP header. Possible values are described in Table 9.7 ⇨. If your IP network uses diferentiated services, you can also define the DSCP (differentiated services codepoint) for the RTP packets. The DSCP is the first six bits in the TOS octet. **NOTE: VoipUseIpStack must be 0 (default).**
VoipRtcpTos=<num> Enter a value between 0 and 255 to set the TOS (type of service) field in the RTCP packet IP header. Possible values are described in Table 9.7 ⇨. If your IP network uses diferentiated services, you can also define the DSCP (differentiated services codepoint) for the RTCP packets. The DSCP is the first six bits in the TOS octet. **NOTE: VoipUseIpStack must be 0 (default).**

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipPCMPacketInterval=<int> This parameter changes the default interval for PCM codecs (G.711, G.726). That means the VoipTxm factor is mulipied using this interval: For 16-channel chips: 0 = 20ms (default) 1 = 5 ms 2 = 10 ms 3 = 20 ms For 8-channel chips: 0 = 10ms (default)) 1 = 5 ms 2 = 10 ms 3 = 20 ms
VoipCallGroup=<name> All outgoing VoIP calls for VoIP profiles with the same VoipCallGroup name are distributed cyclically to these profiles.
VoipOverflow=<name> When the value entered in VoipMaxChan is reached, all overflow calls will be sent to the profile defined here. An alternative VoIP profile can also be used if the default profile can no longer be used as a result of poor quality.
VoipDJBufMinDelay=<count> Enter a value in milliseconds (0-320) to set a minimum jitter buffer limit (default 35). For fax transmission (t.38) it is fixed to 200ms. **NOTE: VoipDJBufMaxDelay must be greater than VoipDJBufMinDelay.**
VoipDJBufMaxDelay=<count> Enter a value in milliseconds (0-320) to set a maximum jitter buffer limit (default 150). For fax transmission (t.38) it is fixed to 200ms. **NOTE: VoipDJBufMaxDelay must be greater than VoipDJBufMinDelay.**
VoipDJBufOptFactor=<count> Enter a value between 0 and 13 to set the balance between low frame erasure rates and low delay (default 7).
VoipConnBrokenTimeout=<sec> An entry is generated in the protocol.log file and the connection is terminated after a connection broken exists for the number of seconds entered (default 90). If `0` is entered, no entry will be generated and the connection will not be terminated.

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipTcpKeepAlive=<mode> Enter yes (default) to send the RoundTripDelayRequest message every 10 seconds (necessary for long calls with firewalls using TCP aging).
VoipIntrastar=<mode> Enter Yes to activate the IntraSTAR feature. When the IP connection results in poor quality, an ISDN call is sent to the peer and the voice data is automatically transmitted via ISDN.
VoipBrokenDetectionTimeout=<ms> When this parameter is set, the system recognizes an interruption in the transmission of RTP/RTCP data in the VoIP connection following the set number of milliseconds. This parameter is necessary to set up an IntraSTAR call immediately when the IP connection is disrupted. Bear in mind that VoipSilenceSuppression=No must appear in the VoIP profile.
VoipAutoRtpAddr=<mode> Some application scenarios require automatic RTP IP address and port recognition for VoIP calls, for example if a firewall or NAT changes the IP address of incoming RTP data. Enter Yes to activate automatic recognition (default No).

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipAGC=<x y z> This parameter allows automatic gain control of input signals from PSTN or IP. Enabling this feature compensates for near-far gain differences: `x` - direction (`0` for signals from TDM, `1` for signals from IP) `y` - gain slope (controls gain changing ratio in -dBm/sec, values 0 to 31, default 0) `z` - target energy (determines attempted signal energy value in -dBm, values 0 to 63, default 19 Gain Slope: 0 - 00.25dB 1 - 00.50dB 2 - 00.75dB 3 - 01.00dB 4 - 01.25dB 5 - 01.50dB 6 - 01.75dB 7 - 02.00dB 8 - 02.50dB 9 - 03.00dB 10 - 03.50dB 11 - 04.00dB 12 - 04.50dB 13 - 05.00dB 14 - 05.50dB 15 - 06.00dB 16 - 07.00dB 17 - 08.00dB 18 - 09.00dB 19 - 10.00dB 20 - 11.00dB 21 - 12.00dB 22 - 13.00dB 23 - 14.00dB 24 - 15.00dB 25 - 20.00dB 26 - 25.00dB 27 - 30.00dB 28 - 35.00dB 29 - 40.00dB 30 - 50.00dB 31 - 70.00dB

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipVoiceVolume=<num> The volume of VoIP calls coming from the Ethernet. The range is 0-63. The default value of 32 is 0 dB.
VoipInputGain=<num> The volume of VoIP calls coming from ISDN or mobile. The range is 0-63. The default value of 32 is 0 dB.

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipQualityCheck=<type minsamples limit recovertime> type Enter one of the following: ASR1, ASR2, RoundTripDelay, Jitter or FractionLost **When type is ASR1 or ASR2**: minsamples Minimum number of calls for which ASR shall be calculated with: limit A value between 0 and 100 recovertime Seconds to block the profile. **When type is RoundTripDelay**: minsamples Minimum number of seconds RTD must be above: limit The highest acceptable value for RTD (in milliseconds) recovertime Seconds to block the profile. **When type is Jitter**: minsamples Minimum number of seconds jitter must be above: limit The highest acceptable value for jitter (in milliseconds) recovertime Seconds to block the profile. **When type is FractionLost**: minsamples Minimum number of seconds FL must be above: limit The highest acceptable value for FL (percentage between o and 100) recovertime Seconds to block the profile **NOTE: If you base VoipQualityCheck on the ASR values: During setup, calls are calculated as not connected, which lowers the number of connected calls.** Example: If minsamples is set at 20, with a limit of 80%, 4 calls in the setup phase will lower the ASR of the previous 20 calls to 80% and the profile will be blocked.
VoipECE=<mode> Enter yes (default) to set ITU G. 168 echo cancellation. Enter no to disable echo cancellation.

Table 9.6 Customized Parameters: VoIP Quality *(continued)*

VoIP Quality Parameters
VoipEcl=<ms> This parameter defines the required tail length for echo cancelation. The following values in ms are possible: 32 64 (default) 128
VoipT301=<sec> An outgoing VoIP calls will be canceled in the state of Alerting (for H323) or Ringing (for SIP) if the number of seconds entered has passed and there is no response from the IP or VoIP carrier.

VoipT303=<sec>
If this parameter is entered in a SIP profile, transmission of the INVITE is canceled after the number of seconds entered has passed. The call can then be redirected, for example to PSTN. This improves the reliability of the system when an IP or VoIP carrier's service fails.
EXAMPLE:
`Redirect340DF:=A`
`MapAllA=9`
`[Voip:DF]`
`.....`
`VoipT303=5`

VoipT304=<sec> An outgoing VoIP calls will be canceled in the state of Setup Acknowledge (for H323) or Trying (for SIP) if the number of seconds entered has passed and there is no response from the IP or VoIP carrier.
VoipT310=<sec> An outgoing VoIP calls will be canceled in the state of Call Proceeding (for H323) or Session Progress (for SIP) if the number of seconds entered has passed and there is no response from the IP or VoIP carrier.

The following specifications for Quality of Service correspond with RFC791 and RFC1349.

Table 9.7 Quality of Service Values

Bit Distribution	0	1	2	3	4	5	6	7
	Precedence			TOS				MBZ
Bit	Description							
0-2	Precedence							
3	TOS: 0=normal delay, 1=low delay							
4	TOS: 0=normal throughput, 1=high throughput							
5	TOS: 0=normal reliability, 1=high reliability							

Table 9.7 Quality of Service Values *(continued)*

6	TOS: 0=normal service, 1=minimize monetary cost
7	MBZ: must be 0 (currently not used)
Precedence	Description
111	Network control
110	Internetwork control
101	CRITIC/ECP
100	Flash override
011	Flash
010	Immediate
001	Priority
000	Routine

9.5 COMPRESSION PARAMETERS

The following parameters are for RTP multiplexing, which aggregates RTP packets (voice user data) for individual VoIP calls into a packet. The header (for Ethernet, IP, UDP and RTP) is sent only once for all calls instead of for each individual call. The relationship between header and payload benefits the payload when several calls occur simultaneously. This compression does not result in any loss in voice quality.

This feature is possible with a Teles peer and requires the following entries in the VoIP profile:

Table 9.8 Customized Parameters: VoIP Compression

VoIP Compression Parameters
VoipAggRemoteRtpPort=<port> Enter the port for the VoIP peer that is the first RTP port. The next port is always the corresponding RTCP port. The port that is two numbers higher will be used for the next VoIP channel. Default 29000.

VoipAggRemoteDataPort=<port>
`VoipAggRemoteDataPort=29500`
Enter the port for the VoIP peer that is used for aggregated packets (compressed data). Default: 29500.

VoipAggOwnDataPort=<port>
`VoipAggOwnDataPort=29500`
Enter the own port number used for aggregated packets. Default: 29500.

VoipAggRemoteRtpPortSpacing=<count> Defines the space between the ports used for the peer’s individual RTP streams (default 2).

9.6 FAX/MODEM PARAMETERS

Table 9.9 Customized Parameters: VoIP Fax

VoIP Fax/Modem Parameters
VoipFaxTransport=<int> Enter `2` and signaling will switch to G.711a (framesize 40ms) when the peer cannot handle fax transmission with T.38. The codec will change when the system detects a fax or modem connection on the channel. `0` = disabled (default); `1` = relay. T.38 is always used. **NOTE: Bear in mind that if T.38 is defined in the `VoipCompression=` line of the VoIP profile, the system will switch only when it detects a modem connection. Fax calls will still be transmitted using T.38.**
VoipFaxBypassPayloadType=<num> Defined the payload type for a fax's RTP packets when T.38 is not used (default 102).
VoipFaxMaxRate=<num> If the peer does not support auto negotiation or has a fixed transmission rate, you can define the fixed rate: 0 - 2400 Bit/sec 1 - 4800 2 - 7200 3 - 9600 4 - 12000 5 - 14400 (default) EXAMPLE: `VoipFaxMaxRate=5`
VoipFaxECM=<mode> You can use this parameter to disable the error correction mode for fax transmission: `yes`=enabled (default), `no`=disabled.
The following parameters are responsible to set the modem transport method if a modem connection is detected.
VoipV21Transport=<mode> `0`=disabled (must be set to 0).

Table 9.9 Customized Parameters: VoIP Fax *(continued)*

VoIP Fax/Modem Parameters
VoipV22Transport=<mode> 0=disabled, 2=bypass (default).
VoipV23Transport=<mode> 0=disabled, 2=bypass (default).
VoipV32Transport=<mode> 0=disabled, 1=relay (default), 2=bypass .
VoipV34Transport=<mode> 0=disabled, 1=fallback to v32, 2= bypass (default).

9.7 DTMF PARAMETERS

Table 9.10 Customized Parameters: VoIP DTMF

VoIP DTMF Parameters
VoipIBSDetectDir=<int> Enter **1** and DTMF tones (and all other inband signaling) will be detected from the Ethernet side. Enter 0 for DTMF tones to be detected from the PCM side (default). DTMF tones from the Ethernet side are transmitted to the host as ISDN dialing information only if 1 is entered. In this case, VoipDtmfTransport should be 1 or 3. **NOTE: If 1 is entered, fax detection is not supported.**
VoipDtmfTransport=<int> 0 (H323) = DTMF relayed with H.225 signaling information. 0 (SIP) = DTMF relayed with SIP INFO. 1 = DTMF and MF taken from audio stream and relayed to remote. 2 (default) = DTMF and MF kept in audio stream and not relayed. 3 = DTMF and MF taken from audio stream and relayed to remote as per RFC2833. 4 (SIP only) = SIP INFO messages will be relayed as DTMF and MF.
VoipDtmfFallback=<int> If VoipDtmfTransport=3 is set and the peer does not support DTMF transmission according to RFC 2833, the following settings apply: 2 = automatic fallback to inband 0 = automatic fallback to signaling messages (default)
VoipRFC2833PayloadType=<num> This parameter changes the DTMF payload type. The default value is 96, a common value is 101.
VoipMinDigitOnTime=<ms> Defines the minimum length of DTMF tones, to ensure DTMF tone detection. Default 0.
VoipMinInterDigitTime=<ms> Sets a time interval for DTMF tone detection. Default 0.

10 SYSTEM MAINTENANCE AND SOFTWARE UPDATE

10.1 CONFIGURATION ERRORS

When typographical errors are made in the configuration files, an entry appears in the `protocol.log` when the configuration is activated. This entry includes the line number and its contents.

10.2 STATUS AND ERROR MESSAGES

The `protocol.log` file – assigned as the file for logging the protocol in the configuration file (`ActionLog=`*file*) – contains information on all activities within the system. In the example below, you can see that all activities are recorded beginning with the date and time. If functions were activated by key combinations from terminal devices you can identify these along with the service ID.

```
16.05.06-11:51:31,[990]Start STATUS - TELES.iGATE V11.7a (007f)
16.05.06-12:10:57,[01A]ERR: Layer1
16.05.06-12:10:58,[000]ERR: OK
16.05.06-12:10:58,[010]ERR: OK
16.05.06-12:12:06,Remote Control from IP 192.168.1.2
16.05.06-12:12:06,Remote Control: OK
16.05.06-12:12:16,Activate Configuration System
16.05.06-12:16:26,Remote Control Terminated
16.05.06-14:00:00,Activate Configuration Night2
16.05.06-14:00:00,Time Switch Operation
16.05.06-18:00:00,Activate Configuration Night3
16.05.06-18:00:00,Time Switch Operation
```

Table 10.1 Event Log Messages

Message	NMS	Definition
Status Program		
[990] Start STATUS	X	TELES system software and status program have been started.
System Start		
[999] System-Boot	X	System restarted by timer.
[999] Remote Control: Reboot		System restarted by remote administration command.
Configuration Changes		
Activate configuration <num> OK		Configuration **<num>** successfully loaded. Initiator displayed in next line.
Activate configuration <num> failed [<err>]		Configuration **<num>** could not be loaded.

Table 10.1 Event Log Messages *(continued)*

Message	NMS	Definition
Remote Control: Date & Time changed		Date and/or time were changed via remote administration.
Time Switch Operation		The configuration change was made by the timer.
Remote Administration		
Remote Control from <peer>, <RemoteCode>, <service>, 0		Remote administration access from number or IP address.
Remote Control: OK		Successful remote administration access.
[993]Remote Control: wrong password	X	Remote administration access was denied because of a wrong password.
[994]Remote Control: wrong number	X	Remote administration access was denied because the call originated from an unauthorized number (RemoteOrigination).
Remote Control Terminated <start time>,<end time>, <num>, <RemoteCode>, <service>, 0		Remote administration session from <num> ended. Session length is indicated by start time and end time.
Errors Reported by the Status Program		

Table 10.1 Event Log Messages *(continued)*

Message	NMS	Definition
[<port><i>] ERR: Problem at Port <num>	X	A Layer 1 or Layer 2 error occurred on `<num>`. <i> indicates error type: A Layer 1 error ; Layer 2 error 0 Layer 1&2 operational. 4 RSSI (for mobile only) Should the error persist, a differentiation is possible through 'status of the ports'. If this message appears, status inquiry connections via remote administration are accepted and NMS downloads the protocol.log file. **NOTE: If the RSSI falls below the value configured in the pabx.cfg, the port will shut down automatically.**
Attention: No Callback-Call <num> Arrived		Callback with DTMF: the Callback Provider <num> did not call back within approx. 20 sec. Direct Line Access with DTMF: the call was accepted but disconnected again within x sec. (as defined by MapCallBack-WaitDisc).
Write error		Access to the disk drive on which the data is to be stored was not possible because it is set for read-only, full or because of faulty hardware or software.
[995] Msg-Memory > 75%	X	This message appears when message memory is over 75% full. If this message appears, status inquiry connections via remote administration are accepted and NMS downloads the protocol.log file.

The following options are available for monitoring the iGATE 4 Mobile Boards’ status or the status of each mobile channel. You can access status information through data recorded in the `protocol.log` file or in the **Layer 1** column in the GATE Manager’s **Port Status** window.

Table 10.2 Status Entries

Definition	Protocol Log	GATE Manager
mobile channel is in initializing phase		initialising
SIM card carrier module has not been inserted	ERR: SIM-Card	not reg., no sim
Power supply to the iGATE 4 Mobile Board is not available		not reg., no power
SIM card could not log on because of incorrectly configured PIN		wrong PIN 1x wrong PIN 2x
SIM card is logged on, mobile channel is not		not reg.
SIM card is logged on, mobile channel is searching for a base station		sim exists
SIM card is logged on, but barred (e.g. insufficient field strength)	Barred	reg.barred
SIM card is logged on, mobile channel registers as roaming	ERR: OK	roaming
SIM card is logged on, mobile channel is logged on	ERR: OK	registered
No SIM card detected or inserted	ERR: layer 1	no SIM
SIM card is logged off, mobile channel is logged off	ERR: layer 1	on hold
No mobile channel was available for the call.	ERR: No Chan	
Values have fallen below the parameter’s settings; the Mobile channel will be restarted.	ERR: ASR	

The following status and error messages appear in the `protocol.log` file when `ALARM` appears in the VoIP port's subscriber line:

Table 10.3 Protocol Log Status and Error Messages

Message	Definition
System Configuration (a)	
config: <num> duplicate profile	Specified line in pabx.cfg or route.cfg contains duplicate profile.
config: <num> invalid	Specified line in pabx.cfg or route.cfg is invalid.
config: evaluation errcode <num>	Internal error.
Port-Specific Entries	
[<port>]Unblock Port	The <port> has been unblocked. This can occur via remote access for all controller types or automatically via vGATE for mobile channels.
[<port>]Block Port	The <port> has been blocked. This can occur via remote access for all controller types or automatically via vGATE for mobile channels.
[<port>]Restart Port	The <port> has been blocked. This can occur via remote access for all controller types or automatically via vGATE for mobile channels.
Ethernet Interface	
[99d]ERR: emac<num><state>	The Ethernet controller's status is checked every minute and any change in status is noted. <num> Number of the EMAC interface (0 or 1). <state> up Ethernet link is active down Ethernet link is inactive
!resolve ip-address	ARP request for specified IP address failed.
pingcheck failed	Ping to configured server failed for configured amount of time; host might reboot this port.
Voice Packetizer Task (b)	
[<port>]ERR: OK, <count> devices	The number (<count>) of DSPs were loaded during startup without errors. The first VoIP controller appears in [<port>].
[<port>]ERR: init failed	A DSP could not be loaded. This DSP or the first VoIP controller is defined in [<port>].
VP: <channel> <msg>	Voice-packetizer chips report fatal error on specified channel, with specified message.
VoIP (c)	
GK <name> URC	Successful UnRegister from specified gatekeeper.

Table 10.3 Protocol Log Status and Error Messages *(continued)*

Message	Definition
GK <name> GRJ <num>	GatekeeperRequest was rejected
GK <name> RCF	Successful RegistrationRequest (RegistrationConfirm).
GK <name> RRJ <num>	RegistrationRequest was rejected.
GK <name> ARJ <dad> <num>	AdmissionRequest was rejected.
GK <name> !ACF dad	AdmissionRequest was not answered.
GK <name> !GCF	GatekeeperRequest was not answered.
no profile for ipaddress	Incoming VoIP call from specified IP address was rejected due to no matching VoIP profile.
registrar <name>: registration done	Successful registration at SIP registrar.
registrar <name>: wrong auth-type <num>	Registrar does not perform MD5 for authentication.
registrar <name>: gives no nonce	Nonce missing in response from registrar (possible error in registrar configuration).
registrar <name>: registration forbidden	Registration with specified registrar is not allowed.
registrar <name> not answering	Specified registrar does not respond.
voipconn oad->dad broken	Voice codec chips report broken RTP connection.
voip FdInitAll failed <cause>	Internal failure.
voip ISDNListen failed	Internal failure.
voipIpSocketInit failed	Internal failure.
!DNS-lookup <hostname>	DNS lookup for specified host name failed (DNS not activated? Missing or invalid DNS server?).
message from <ip addr> not decodable	H323, ASN1 packet cannot be decoded.
vGATE	
[99]ERR: SimUnit !connect	An outgoing connection to the vGATE Sim Unit could not be established.
[99]ERR: ControlUnit <ip addr> !connect	An outgoing connection to the vGATE Control Unit could not be established.
Number Portability	
[99i]ERR: np !connect	Connection to the iMNP could not be established.
[99i]ERR: np connect <ip addr>	Connection to the iMNP reestablished.

Table 10.3 Protocol Log Status and Error Messages *(continued)*

Message	Definition
System Kernel (e)	
task <name> suspended	specified task was suspended due to internal error; host might reboot this port.
Mail (f)	
cdr !connect <ip addr>	sending CDR: TCP connect to specified IP address failed.
mail !connect <ip addr>	sending e-mail: TCP connect to specified IP address failed.
Radius (g)	
!DNS-lookup <hostname>	DNS lookup for specified host name failed (DNS not activated? Missing or invalid DNS server?).
timeout auth <ip addr>	Authentication request to specified Radius server failed due to timeout.
timeout acnt <ip addr>	Accounting request to specified Radius server failed due to timeout.
!rsp-auth <ip addr>	Response authenticator from specified Radius server was invalid (wrong secret/password?).
!auth <ip addr> <num>	Authentication denied by specified Radius server.
Configuration Errors in the ip.cfg	
Error in ip.cfg line <line>: section [<section_name>] unknown	
Error in ip.cfg line <line>: parameter "<parameter_name>" in [<section_name>] unknown	
Error in ip.cfg line <line>: parameter "<parameter_name>" does not belong to any Section	
There is an error in the NAT Configuration The NAT was not loaded, please check the Configuration for mistakes	
There is an error in the DHCPD Configuration The DHCP SERVER was not loaded, please check the Configuration for mistakes	
There is an error in the ALTQD Configuration The ALTQD SERVER was not loaded, please check the Configuration for mistakes	
There is an error in the FIREWALL Configuration The FIREWALL was not loaded, please check the Configuration for mistakes	
Error in <dsl_interface> Connection failed. Please, connect a cable in the <ethernet> port	
Error in <dsl_interface>: Connection Failed. Please, revise your Username/Password configuration	
Error in <dsl_interface>: Connection Failed. Please, revise the DSL Modem	

10.3 SOFTWARE UPDATE

You may find that you would like to implement features that are only possible with a more recent software version. To update the software on your system, follow these instructions.

Make sure no traffic is running on the system while updating the system. Do not turn the system off during the update.

Check the software version running on your system to make sure the one you want to install is newer. The basic software consists of the following files:

start
netbsdz
netbsdfs.gz
and one of the following:
iGATE GSM: igate.tz1
or

iGATE CDMA: cgate.tz1
or

iGATE UMTS: igate.tz1

These files form a unit and belong to the same software version. To avoid compatibility conflicts, check with TELES service before you update the software.

Upload the new files ONLY via GATE Manager. Do not use any other process (e.g. FTP) to update the software files. This can lead to irreversible damage to the operating system.

Make sure there is enough available memory for the new version. We recommend that you delete unnecessary log files and back-ups. **Do NOT delete or rename existing software files before updating.**

If an error message appears during the update process, no NOT restart or turn off the system! Make a note of the error message and the update steps that have been taken and contact TELES service.

Once the files have been completely transferred, check the file size and reboot the system. As soon as you can reach the system via GATE Manager again, check the version number of the running software.

An update of the following optional function modules (see Chapter 12 ➩) occurs in the same way. Make sure the file extension has the same running number as that of the file on the system:

- HTTP user interface:
  httpd.tz2
  httpd.izg
- DNS forwarder:
  dnsmasg.tz2
- SNMP agent:
  snmpd.tz0
- IP update:
  ipupdate.tz2

The only exception is that you must shut down the modules that have *.izg files before updating. To shut down these modules, change the name of or delete the corresponding *.tz* file and restart the system.

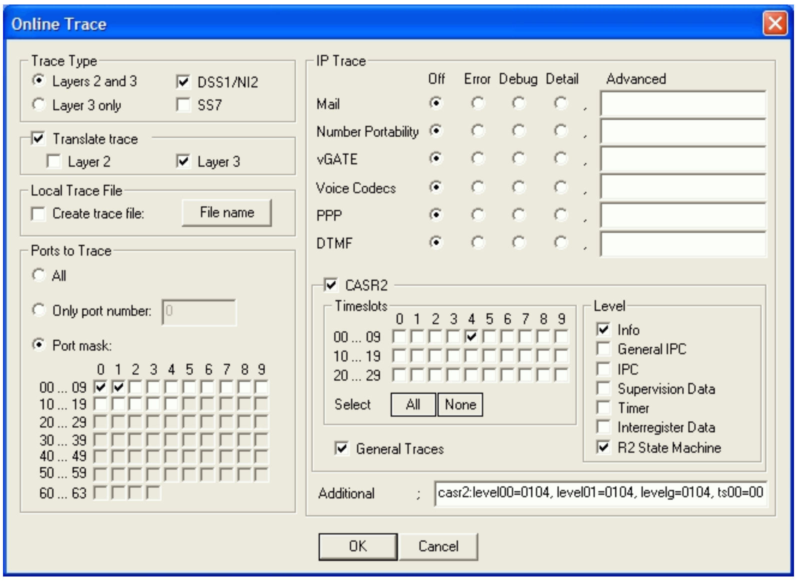
Following transfer of the *.izg file, you must rename the *.tz.* file again and restart the system.

10.4 TRACE

During operation, the trace readouts of the iGATE can be saved in a file or transmitted with remote maintenance directly. The trace options must be turned on in the GATE Manager (offline or online trace) or via FTP raw commands (see Chapter 4.11.2 ➯). Trace results presented here are for PRI,VoIP, GSM/CDMA/UMTS interfaces and for the following services in various levels:

Table 10.4 Trace Options

Option	Definition
Mail	Output for all SMTP packets.
NumberPortability	Output of all packets for communication with the iMNP.
vGATE	Output of all packets for communication with the vGATE.
VoiceCodecs	Output of RTCP information described under VP module.
PPP	Output of PPP connection information.
DTMF	Output for DTMF tone recognition.
Remote	Output for GATE Manager and NMS communication.



Trace Type
● Layers 2 and 3 ☑ DSS1/NI2
○ Layer 3 only □ SS7

☑ Translate trace
□ Layer 2 ☑ Layer 3

Local Trace File
□ Create trace file:

Ports to Trace
○ All
○ Only port number: 0
● Port mask:

	0	1	2	3	4	5	6	7	8	9
00 ... 09	☑	☑	□	□	□	□	□	□	□	□
10 ... 19	□	□	□	□	□	□	□	□	□	□
20 ... 29	□	□	□	□	□	□	□	□	□	□
30 ... 39	□	□	□	□	□	□	□	□	□	□
40 ... 49	□	□	□	□	□	□	□	□	□	□
50 ... 59	□	□	□	□	□	□	□	□	□	□
60 ... 63	□	□	□	□						

IP Trace

	Off	Error	Debug	Detail	Advanced
Mail	●	○	○	○ ,	
Number Portability	●	○	○	○ ,	
vGATE	●	○	○	○ ,	
Voice Codecs	●	○	○	○ ,	
PPP	●	○	○	○ ,	
DTMF	●	○	○	○ ,	

☑ CASR2

Timeslots

	0	1	2	3	4	5	6	7	8	9
00 ... 09	□	□	□	□	☑	□	□	□	□	□
10 ... 19	□	□	□	□	□	□	□	□	□	□
20 ... 29	□	□	□	□	□	□	□	□	□	□

☑ General Traces

Level
☑ Info
□ General IPC
□ IPC
□ Supervision Data
□ Timer
□ Interregister Data
☑ R2 State Machine

Additional ; casr2:level00=0104, level01=0104, levelg=0104, ts00=00

Figure 10.1 GATE Manager: Offline Trace Activation Window

iGATEs offer two different types of trace:

- Online - trace information is immediately displayed in the GATE Manager's trace window.
- Offline - trace information is written to a file on the iGATE.

iGATE systems create trace files when the TraceLog=file entry is present in the pabx.cfg. Traces can be activated via remote administration (GATE Manager or FTP).

Table 10.5

Please bear in mind that the volume of trace readouts can grow quite large, so that faulty transmission of the trace data may result with remote maintenance. A trace at full capacity can cause the system to crash.

Trace Output Format

The following entries appear at the beginning and end of each trace:

- DD.MM.YY-hh:mm:ss.ss, Start
- DD.MM.YY-hh:mm:ss.ss, End
  - DD = day
  - hh = hour
  - MM = month
  - mm = minute
  - YY = year
  - ss.ss = hundredths of seconds

Traces appear in the following format:

- [<hh:mm:ss>] <module>[<port>]: <trace>
- <module>
  - s = send for PRI/BRI or mobile ports
  - r = receive for PRI/BRI or mobile ports
  - x = send to VoIP destinations
  - y = receive from VoIP destinations
  - i = information messages and internal trace outputs between VoIP and the other interfaces (ISDN, mobile)
  - a = VoIP controllers RTCP output
  - m = mail output
  - g = remote output
- <port>
  - port number (controller number in the pabx.cfg) or 255 if a service is used
- <trace>
  - output in the defined syntax for the module

10.4.1 ISDN TRACE OUTPUT

Trace output for DSS1 and SS7 are in hexadecimal notation. You can use the external tool TraceView.exe to translate offline trace output. You will find the tool in the **Software** folder on the enclosed CD. The GATE Manager's trace window can also display translated online traces.

Example: The following example shows an untranslated DSS1 trace:

```
17.05.06-09:54:40,Start 11.7a (L3)
[09:55:14.58] r[00]: 00 01 02 02 08 02 00 02 05 04 03 80 90 a3 18 03 a1 83 81 6c 02 81 31 70 06 81 31 32 33
34 35 7d 02 91 81
[09:55:14.58] s[00]: 02 01 02 04 08 02 80 02 0d 18 03 a9 83 81
[09:55:14.58] s[01]: 00 01 a8 9a 08 02 00 46 05 04 03 80 90 a3 18 03 a1 83 89 6c 02 81 31 70 06 81 31 32 33
34 35 7d 02 91 81
[09:55:14.58] r[01]: 02 01 9a aa 08 02 80 46 0d 18 03 a9 83 89
[09:55:14.86] r[01]: 02 01 9c aa 08 02 80 46 01
[09:55:14.86] s[00]: 02 01 04 04 08 02 80 02 01
[09:55:16.73] r[01]: 02 01 9e aa 08 02 80 46 07 29 05 05 07 01 09 33 4c 07 01 81 31 32 33 34 35
[09:55:16.73] s[01]: 00 01 aa a0 08 02 00 46 0f
[09:55:16.73] s[00]: 02 01 06 04 08 02 80 02 07 29 05 05 07 01 09 32 4c 07 01 81 31 32 33 34 35
[09:55:16.73] r[00]: 00 01 04 08 08 02 00 02 0f
[09:55:44.30] r[00]: 00 01 06 08 08 02 00 02 45 08 02 80 90
[09:55:44.35] s[01]: 00 01 ac a0 08 02 00 46 45 08 02 80 90
[09:55:46.71] r[01]: 02 01 a0 ae 08 02 80 46 4d
[09:55:46.71] s[01]: 00 01 ae a2 08 02 00 46 5a
[09:55:46.71] s[00]: 02 01 08 08 08 02 80 02 4d
[09:55:46.71] r[00]: 00 01 08 0a 08 02 00 02 5a
17.05.06-09:51:33,End
```

10.4.2 GSM/CDMA/UMTS TRACE OUTPUT

The trace output for GSM appears in hexadecimal notation. Its format is the same as that for ISDN output. Table 10.6 ⇨ and Table 10.7 ⇨ describe the contents of GSM trace output.

Table 10.6 Request Messages to the GSM Module

Hex Value	Description
00	Setup
01	Connect
02	Disconnect
03	SMS
04	DTMF
05	Set Config
06	Get Config
07	LED
08	Restart
09	Switch SIM

Table 10.7 Incoming, Indication Message from the GSM Module

Hex Value	Description
0B	Alert
0C	Voice Indication
0D	Connect
0E	DTMF
0F	Setup
10	Disconnect
11	SMS
12	SMS Confirmation
13	Error
16	Get Config Confirmation
18	Dial-End Call Proceeding
19	USSD
1A	Restart Indication

Example: The following example shows a GSM call through the fourth GSM controller:

```
Status Request
[14:57:51.80] s[04]: 06
Status Information:
[14:57:51.80] r[04]: 16
Setup Request:
[14:57:52.29] s[04]: 00 4c 93 04 00 00 00 35 36 36 37 00 35 38 2c 36 34 36 2c 33 30 2c 2c 2c 30 2c 2c 2c
30 2c 32 36 32 2c 30 37 2c 00 72 64 09 75 70 20 7b 64 35 7d 20 27 2e 2e 2b 43 43 45 44 3a 20 32 36 32 2c
30 37 2c 34
Dial End:
[14:57:55.47] r[04]: 18
Alert:
[14:57:55.63] r[04]: 0b
Connect Indication:
[14:57:56.63] r[04]: 0d
Disconnect Request:
[14:59:54.13] s[04]: 02 4c 93 00
Disconnect Indication:
[14:59:54.19] r[04]: 10
```

10.4.3 VOIP TRACE OUTPUT

As described above in Chapter 10.4 ➯, there are four modules for VoIP traces. The groups x (send), y (receive) and i (information and internal output) appear when a Layer2 or Layer3 offline or online trace is started. Group a (RTCP output) only appears when the module Voice Codecs is active.

Particularly in the case of VoIP connections (protocols H.323 and SIP), the trace output is quite extensive and abbreviations make it difficult to keep track of the results. The following list contains a description of H.323 output.

Output for the signaling protocol SIP is transmitted in ASCII and translated for better legibility. Since they are displayed unabridged, no description is necessary. Information and internal output traces correspond with the H.323 output and are described in the following tables. For ENUM, please refer to Chapter 10.4.3.5 ⇨.

In general, the following rules apply for this trace output:

Table 10.8 H.323 Output

Packet	Description
h225	H.225-protocol messages.
h245	H.245-protocol messages.
pstn	Messages of the internal protocol interface that provides the interface to the other interfaces PRI, BRI and GSM.
rcv	Coming from the IP network or the internal protocol interface; appears with <dir> in the trace lines.
snd	Sending to the IP network or the internal protocol interface; appears with <dir> in the trace lines.

The information is thoroughly analyzed where it is received (all rcv messages).

10.4.3.1 INTERFACE IP NETWORK

Establish H.323 Session

Usually there is trace output that displays a new H.323 session. The direction is crucial (whether the call is going into or coming out of the IP network).

```
h225connect to <ip address> cr <cr> s <si>
h225accept from <ip address> s <si>
```

Table 10.9 H.323 Session

Trace Output	Description
connect to	Outgoing VoIP call
accept from	Incoming VoIP call
<ip address>	Peer's IP address
cr <cr>	Call reference (corresponds with the internal protocol interface's PSTN call reference)
s <si>	Session ID

H.225 Signaling Output

The following trace results are for a call coming from the IP network. rcv will appear at <dir> and signifies the direction:

```
h225<dir> tpkt msg 0x<mt> h225cr <cr> addr <ip address>
```

Table 10.10 H.225 Signaling

Trace Output	Description
<mt>	The ETS message type in hexadecimal; can consist of values listed in Table 10.11 ⇨.
<hcr>	H.225 call reference in hexadecimal (does not have to be unique when calls come from multiple peers).
<ip address>	The peer's IP address.

Table 10.11 ETS Message Types

Hex Value	Message Type
1	Alerting
2	Call Proceeding
3	Progress
5	Setup
7	Connect
D	Setup Acknowledge
5A	Release Complete
62	Facility
6E	Notify
7B	Information
7D	Status

The following lines show the packet contents in detail:

```
h225 decode rc 0, q931 msg 0x<mt> = 0, len <length>
h225<type> <mt> voipcfg addr <ip address> rc 0 compr <codec>
h225<type> <mt> h225cr <hcr> FS:<bool> (<codec>,<ip address>,<port>) TUNN:<bool>
H245:<bool>(<ip address>,<port>)
h225<type> <mt> h225cr <hcr> cr <cr>
```

Table 10.12 Incoming VoIP Calls

Trace Output	Description
<mt>	Message type in hexadecimal as per ETS standard (see Table 10.11 ➩) or written out as a name.
len <length>	Packet length in bytes.
h225<type>	H.225 `rcv` or `send`; received or sent from the IP network.
addr <ip address>	Peer's IP address.
compr <codec>	Peer's compression list (see Table 10.13 ➩).
FS<bool>	FastStart offered in the signaling packet or not.

Table 10.12 Incoming VoIP Calls *(continued)*

Trace Output	Description
(<codec>,	Lists codecs offered (seeTable 10.34 ⇨).
<ip address>,	Peer's IP address for RTP data.
<port>)	Peer's port for RTP Data.
Tunn<bool>	Shows whether or not tunneling is offered as a signaling variant.
H245<bool>	Shows an extra H.245 session.
(ip address,	Peer's IP address.
port)	Peer's port.
h225cr <hcr>	H.225 message's call reference (does not have to be unique when calls come from multiple VoIP peers).
cr <cr>	Internal call reference (always unique for the call).

Table 10.13 Compression Codecs Used

Synonym	Codec
A	G.711Alaw64k
B	G.711Ulaw64k
C	G.7231
D	G.728
E	G.729
F	gsmFullRate
G	T.38fax
O	G.729A
P	G.72616
Q	G.72624
R	G.72632
S	G.729B
T	G.729AB
U	G.729E

Table 10.13 Compression Codecs Used *(continued)*

Synonym	Codec
V	G.723L
W	Transparent
X	G.721
Y	iLBC20
Z	iLBC30

When the call is sent in the direction of the IP network, the trace will include only the most important information:

```
h225<type> <mt1> dad <num> cr <cr>
```

Table 10.14 Calls to the IP Network 1

Trace Output	Description
<mt>	Message type written out; if a decimal number appears here, it will be translated as per Table 10.11 ⇨.
<num>	Called party number.
<cr>	Call reference.

Or:

```
h225<type> callproc typ <mt> cr <cr>
```

Table 10.15 Calls to the IP Network 2

Trace Output	Description
<mt>	The ETS message type in hexadecimal.
<cr>	Call reference.

RTP/RTCP Output

The RTP/RTCP output displays whether the signaling information corresponds with the contents of the compression chips. The output occurs when a media channel is set up or torn down:

```
rtp start cr <cr> ch <ch> li <li> ri <ri> st <st> fx <fx> cp <comp> txm <factor>
```

Table 10.16 RTP/RTCP Output

Trace Output	Description
<cr>	Call reference.
<ch>	The internal media channel used.
<li>	`1` appears when the local RTP address (and port) has been defined.
<ri>	`1` appears when the remote RTP address (and port) have been established.
<st>	`0` appears if the channel's voice packetizer has not yet been started. `1` appears if the voice packetizer can receive, but not send. `2` appears when the voice packetizer can receive and send.
<fx>	`1` appears when T.38 (fax) is used, otherwise 0.
<comp>	The codec used, as per Table 10.13 ⇨.
<factor>	Multiplication factor for default frame size (20ms, 30 ms for G.723).

```
rtp stop cr <cr>1 ch <ch>
```

Table 10.17 RTP Stop Message

Trace Output	Description
<cr>	Call reference.
<ch>	The internal media channel used.

Table 10.18 RTP Packet Statistics

Trace Output	Description
<ch>	The internal media channel used.
<byte>	The call's received or sent bytes.

```
rtcp <ch>: SR <dir> pc <pc> oc <oc> ji <ji> rt <rt> fl <fl> cl <cl>
```

Table 10.19 RTCP Packet Statistics

Trace Output	Description
<ch>	The internal media channel used.
SR<dir>	Rx sender report (received) is more interesting, since it comes from the peer. Tx sender report (transmitted).
<pc>	Packet count (number of packets transmitted/received).
<oc>	Octet count (number of octets transmitted/received).
<ji>	Delay jitter [msec].
<rt>	Round-trip local<->remote, round-trip delay [msec].
<fl>	Fraction lost: Fraction of packets lost [8lsb].
<cl>	Cumulative lost: number of lost packets [24lsb].

The following output shows the jitter buffer status:

```
a[<controller>]: <VoIPcodecChipType> ch <ch> jitter buffer n1 n2 n3n4 n5 n6 n7 n8
```

Table 10.20 Jitter Buffer Status

Trace Output	Description
n1	SteadyStateDelay in milliseconds

Table 10.20 Jitter Buffer Status *(continued)*

Trace Output	Description
n2	NumberOfVoiceUnderrun
n3	NumberOfVoiceOverrun
n4	NumberOfVoiceDecoderBfi (bfi = bad frame interpolation)
n5	NumberOfVoicePacketsDropped
n6	NumberOfVoiceNetPacketsLost
n7	NumberOfIbsOverrun (ibs = in band signaling)
n8	NumberOfCasOverrun

An RTP connection has ended when the following trace output appears:

```
a[<controller>]: <VoIPcodecChipType> stop ch=<ch>
```

Table 10.21 RTP Stop Message (VP Module)

Trace Output	Description
<ch>	The internal media channel used.

The following output results when the codec changes for a fax connection:

```
a[<controller>]: ac49x ch <ch> fax/data n1 n2 n3
```

Table 10.22 Codec Change for Fax

Trace Output	Description
n1	Fax bypass flag: 0 Voice, data bypass or fax relay 1 Fax bypass
n2	Signal detected on decoder output (see Table 10.23)
n3	Signal detected on encoder input (see Table 10.23)

Table 10.23 faxordatasignalevent

Value	Definition	Description
0	SILENCE_OR_UNKNOWN	Undefined (unknown signal or silence)
1	FAX_CNG	CNG-FAX (calling fax tone, 1100 Hz)
2	ANS_TONE_2100_FAX_CED_OR_MODEM	FAX-CED or modem-ANS (answer tone, 2100 Hz)
3	ANS_TONE_WITH_REVERSALS	ANS (answer tone with reversals)
4	ANS_TONE_AM	ANSam (AM answer tone)
5	ANS_TONE_AM_REVERSALS	ANSam (AM answer tone with reversals)
6	FAX_V21_PREAMBLE_FLAGS	FAX-V.21 preamble flags
7	FAX_V8_JM_V34	FAX-V.8 JM (fax call function, V.34 fax)
8	VXX_V8_JM_VXX_DATA	V.XX-V.8 JM (data call function, V-series modem)
9	V32_AA	V.32 AA (calling modem tone, 1800 Hz)
10	V22_USB1	V.22 USB1 (V.22(bis) unscrambled binary ones)
11	V8_BIS_INITIATING_DUAL_TONE	V.8bis initiating dual tone (1375 Hz and 2002 Hz)
12	V8_BIS_RESPONDING_DUAL_TONE	V.8bis responding dual tone (1529 Hz and 2225 Hz)
13	VXX_DATA_SESSION	V.XX data session
14	V21_CHANNEL_2	V.21 channel 2 (mark tone, 1650 Hz)
15	V23_FORWARD_CHANNEL	V.23 forward channel (mark tone, 1300 Hz)
16	V21_CHANNEL_1=18	V.21 channel 1 (mark tone, 980 Hz)
17	BELL_103_ANSWER_TONE	Bell 103 answer tone, 2225 Hz
18	TTY	TTY
19	FAX_DCN	FAX-DCN (G.3 fax disconnect signal)

Fax relay is activated for the corresponding channel:

```
a[<controller>]: Ac49xActivateFaxRelayCommand(1) ch <ch> rc <cr>
```

The following output shows various values for fax transmission (see Table 10.24 for a description of the values):

```
a[<controller>]: ac49x ch <ch> faxrelay: n1 n2 n3 n4 n5 n6 n7 n8 n9 n10 n11 n12 n13 n14
```

Table 10.24 Fax Status

Value	Description
n1	UnableToRecoverFlag (0 no, 1 yes)
n2	IllegalHdlcFrameDetectedFlag (...)
n3	FaxExitWithNoMcfFrameFlag
n4	HostTransmitOverRunFlag
n5	HostTransmitUnderRunFlag
n6	InternalErrorFlag
n7	ReceivedBadCommandFlag
n8	TimeOutErrorFlag
n9	TxRxFlag (0 receive, 1 transmit)

Table 10.24 Fax Status *(continued)*

Value	Description
n10	T30State 0 FAX_RELAY_T30_STATE__INITIALIZATION 1 FAX_RELAY_T30_STATE__CNG 2 FAX_RELAY_T30_STATE__CED 3 FAX_RELAY_T30_STATE__V21 4 FAX_RELAY_T30_STATE__NSF 5 FAX_RELAY_T30_STATE__NSC 6 FAX_RELAY_T30_STATE__CSI 7 FAX_RELAY_T30_STATE__CIG 8 FAX_RELAY_T30_STATE__DIS 9 FAX_RELAY_T30_STATE__DTC 10 FAX_RELAY_T30_STATE__NSS 11 FAX_RELAY_T30_STATE__TSI 12 FAX_RELAY_T30_STATE__DCS 13 FAX_RELAY_T30_STATE__CTC 14 FAX_RELAY_T30_STATE__CRP 15 FAX_RELAY_T30_STATE__DCN 16 FAX_RELAY_T30_STATE__PRE_MESSAGE_RESPONSE 17 FAX_RELAY_T30_STATE__POST_MESSAGE_RESPONSE 18 FAX_RELAY_T30_STATE__POST_MESSAGE_COMMAND 19 FAX_RELAY_T30_STATE__VXX 20 FAX_RELAY_T30_STATE__TCF 21 FAX_RELAY_T30_STATE__IMAGE
n11	NumberOfTransferredPages
n12	BadInputPacketId
n13	BadInputPacketTotalSize
n14	FaxBitRate 1 FAX_BIT_RATE__300_BPS 2 FAX_BIT_RATE__2400_BPS 3 FAX_BIT_RATE__4800_BPS 4 FAX_BIT_RATE__7200_BPS 5 FAX_BIT_RATE__9600_BPS 6 FAX_BIT_RATE__12000_BPS 7 FAX_BIT_RATE__14400_BPS

The following output appears when the compression chip recognizes DTMF tones:

```
a[<controller]: ac49x ch <ch> ibs <dtmf> <dir> <mode> <lev> <dur>
```

Table 10.25 DTMF Tone Recognition

Trace Output	Description
`<ch>`	Media channel
`<dtmf>`	Recognized DTMF tone in the stream or as per RFC2833
`<dir>`	Direction 0 Coming from BRI/analog 1 Coming from VoIP
`<mode>`	0 Tone has ended 1 Tone has been recognized
`<lev>`	Signal level in -dBm
`<dur>`	Tone duration

10.4.3.2 INTERNAL PROTOCOL INTERFACE (TO ISDN, MOBILE)

These trace outputs always begin with the keyword `pstn`, followed by the direction and the message type. The message is then either concluded or other information follows:

```
pstn<type> <mt1> dad <num> oad <num> cr <cr> s <si> ch <chan> isdncr<icr>
```

Table 10.26 Internal Protocol Interface

Trace Output	Description
<type>	Direction from (`rcv`) or to (`snd`) the internal protocol interface.
<mt1>	Message type written out; if a decimal number appears, it will be translated as per Table 10.11 ➪.
<num>	`DAD<num>` = called party number, `OAD<num>` = calling party number.

Table 10.26 Internal Protocol Interface *(continued)*

Trace Output	Description
<cr>	Call reference.
<si>	Session ID.
<chan>	Media channel used.
<icr>	Call reference for the internal protocol interface (DSS1).

Output also appears when a call comes from the internal protocol interface and is assigned to a VoIP profile. The characters appear in front of the colon in the routing entry:

```
pstnrcv get_voipcfg <voip profile>
```

Table 10.27 Received from PSTN 1

Trace Output	Description
<voip profile>	Defines the VoIP profile to be used.

Assignment of media channel used for the internal interface and the ISDN call reference for the VoIP call's appears as follows:

```
pstnrcv bchanind cr <cr> ch <chan> isdncr <icr>
```

Table 10.28 Received from PSTN 2

Trace Output	Description
<cr>	Call reference.
<chan>	Media channel used for the internal protocol interface (DSS1).
<icr>	Call reference for the internal protocol interface (DSS1).

10.4.3.3 H.245 MESSAGES

The following trace output is possible:

```
h245<dir>(<tt>) cr <cr>
```

Table 10.29 H.245 Messages

Trace Output	Description
<dir>	The message's direction; `rcv` (incoming from the peer) or `snd` (sent message).
<tt>	H.245 transport type.
<cr>	Internal call reference.

Following this trace output, either a detailed description of the message and its corresponding message type, including negotiating information, or trace output elements that are explained later appear. The most important message types that contain further information elements are as follows:

```
... TerminalCapabilitySet peer=<comp> cfg=<comp>
... TerminalCapabilitySet <comp>
```

Table 10.30 Codec Used

Trace Output	Description
<comp>	List of compression codecs offered (see Table 10.13 ➩), the list of the peer's codecs appears behind peer, and `cfg` shows which codecs are defined in the VoIP profile

```
... OpenLogicalChannel cn=<cn> cpr=<comp> sessid=<sid> ctrl=<ip address>:<rtcp port>
... OpenLogicalChannelAck cn=<cn> sessid=<sid> media=<ip address>:<rtp port>
```

Table 10.31 Logical Channel Parameters

Trace Output	Description
<cn>	H.245 channel number per H.225 connection.
<sid>	Session ID.
<comp>	Codec used (see Table 10.13 ⇨).
<ip address>	Protocol peer IP address.
<rtcp port>	Port used for the protocol RTCP.
<rtp port>	Port used for the protocol RTP.

The trace output is as follows when the message type is not translated or is ignored:

```
h245<dir>(<tt>) cr <cr> unknown msg <hmt> <hmi>
```

Table 10.32 H.245 Parameters

Trace Output	Description
hmt	The H.245 message type (multimedia system control message type), (Table 10.33 ⇨).
hmi	The H.245 message ID (see Table 10.34 ⇨, Table 10.35 ⇨, Table 10.36 ⇨, Table 10.37 ⇨).

Table 10.33 Multimedia System Control Message Types

ID	Message
0 (Table 10.34 ⇨)	Request
1 (Table 10.35 ⇨)	Response
2 (Table 10.36 ⇨)	Command
3 (Table 10.37 ⇨)	Indication

Depending on the system control message type, one of the following message IDs appear:

Table 10.34 Message IDs for Request Message

ID	Message
0	NonStandard
1	MasterSlaveDetermination
2	TerminalCapabilitySet
3	OpenLogicalChannel
4	CloseLogicalChannel
5	RequestChannelClose
6	MultiplexEntrySend
7	RequestMultiplexEntry
8	RequestMode
9	RoundTripDelayRequest
10	MaintenanceLoopRequest
11	CommunicationModeRequest
12	ConferenceRequest
13	MultilinkRequest
14	LogicalChannelRateRequest

Table 10.35 Message IDs for Response Message

ID	Message
0	NonStandard
1	MasterSlaveDeterminationAck
2	MasterSlaveDeterminationReject
3	TerminalCapabilitySetAck
4	TerminalCapabilitySetReject
5	OpenLogicalChannelAck
6	OpenLogicalChannelReject

Table 10.35 Message IDs for Response Message *(continued)*

ID	Message
7	CloseLogicalChannelAck
8	RequestChannelCloseAck
9	RequestChannelCloseReject
10	MultiplexEntrySendAck
11	MultiplexEntrySendReject
12	RequestMultiplexEntryAck
13	RequestMultiplexEntryReject
14	RequestModeAck
15	RequestModeReject
16	RoundTripDelayResponse
17	MaintenanceLoopAck
18	MaintenanceLoopReject
19	CommunicationModeResponse
20	ConferenceResponse
21	MultilinkResponse
22	LogicalChannelRateAcknowledge
23	LogicalChannelRateReject

Table 10.36 Message IDs for Command Message

ID	Message
0	NonStandard
1	MaintenanceLoopOffCommand
2	SendTerminalCapabilitySet
3	EncryptionCommand
4	FlowControlCommand
5	EndSessionCommand

Table 10.36 Message IDs for Command Message *(continued)*

ID	Message
6	MiscellaneousCommand
7	CommunicationModeCommand
8	ConferenceCommand
9	h223MultiplexReconfiguration
10	NewATMVCCommand
11	MobileMultilinkReconfigurationCommand

Table 10.37 Message IDs For Indication Message

ID	Message
0	NonStandard
1	FunctionNotUnderstood
2	MasterSlaveDeterminationRelease
3	TerminalCapabilitySetRelease
4	OpenLogicalChannelConfirm
5	RequestChannelCloseRelease
6	MultiplexEntrySendRelease
7	RequestMultiplexEntryRelease
8	RequestModeRelease
9	MiscellaneousIndication
10	JitterIndication
11	h223SkewIndication
12	NewATMVCIndication
13	UserInput
14	h2250MaximumSkewIndication
15	McLocationIndication
16	ConferenceIndication

Table 10.37 Message IDs For Indication Message *(continued)*

ID	Message
17	VendorIdentification
18	FunctionNotSupported
19	MultilinkIndication
20	LogicalChannelRateRelease
21	FlowControlIndication
22	MobileMultilinkReconfigurationIndication

10.4.3.4 RAS (REGISTRATION, ADMISSION, STATUS)

As a general rule, the most important terminal and gatekeeper messages appear written out with the gatekeeper's IP address (<ip addr>):

```
H225 GatekeeperRequest to <ip addr> (s 131)
H225 GatekeeperConfirm <ip addr>
H225 GatekeeperReject <ip addr> reason <reason>
```

Table 10.38 RAS

Trace Output	Description
<reason>	Gatekeeper reject reason, see Table 10.42 ⇨.

```
H225 GkRegistration to <ip addr>
H225 RegistrationConfirm <ip addr>
H225 RegistrationReject <ip addr> reason <reason>
```

Table 10.39 Gatekeeper 1

Trace Output	Description
<reason>	Registration reject reason, see Table 10.43 ⇨.

```
H225 GkResourcesAvailableIndicate to <ip addr> (<act chan> <max chan>)
H225 ResourcesAvailableConfirm <ip addr>
```

```
H225 GkAdmission cr <cr> to <ip addr>
H225 AdmissionConfirm <ip addr> cr <cr>
H225 AdmissionReject <ip addr> reason <reason>
```

Table 10.40 Gatekeeper 2

Trace Output	Description
<reason>	Admission reject reason, see Table 10.44 ⇨.

```
H225 GkDisengage cr <cr> to <ip addr>
H225 DisengageConfirm <ip addr>
```

```
H225 UnregistrationRequest <ip addr>
H225 GkUnregistrationConf to <ip addr>
```

All other messages appear as follows:

```
H225 unknown msg from Gk <ip addr>: <code>
```

Table 10.41 Gatekeeper 3

Trace Output	Description
<code>	Unknown gatekeeper message, see Table 10.45 ⇨.

Table 10.42 Gatekeeper Reject Reason

ID	Reject Reason
0	resourceUnavailable
1	terminalExcluded
2	invalidRevision
3	undefinedReason
4	securityDenial
5	genericDataReason
6	neededFeatureNotSupported

Table 10.43 Registration Reject Reason

ID	Reject Reason
0	DiscoveryRequired
1	InvalidRevision
2	InvalidCallSignalAddress
3	InvalidRASAddress
4	DuplicateAlias
5	InvalidTerminalType
6	UndefinedReason
7	TransportNotSupported
8	TransportQOSNotSupported
9	ResourceUnavailable
10	InvalidAlias
11	SecurityDenial
12	RullRegistrationRequired

Table 10.43 Registration Reject Reason *(continued)*

ID	Reject Reason
13	AdditiveRegistrationNotSupported
14	InvalidTerminalAliases
15	GenericDataReason
16	NeededFeatureNotSupported

Table 10.44 Admission Reject Reason

ID	Reject Reason
0	CalledPartyNotRegistered
1	InvalidPermission
2	RequestDenied
3	UndefinedReason
4	CallerNotRegistered
5	RouteCallToGatekeeper
6	InvalidEndpointIdentifier
7	ResourceUnavailable
8	SecurityDenial
9	QosControlNotSupported
10	IncompleteAddress
11	AliasesInconsistent
12	RouteCallToSCN
13	ExceedsCallCapacity
14	CollectDestination
15	CollectPIN
16	GenericDataReason
17	NeededFeatureNotSupported

Table 10.45 Unknown Gatekeeper Messages

ID	Message
0	GatekeeperRequest
1	GatekeeperConfirm
2	GatekeeperReject
3	RegistrationRequest
4	RegistrationConfirm
5	RegistrationReject
6	UnregistrationRequest
7	UnregistrationConfirm
8	UnregistrationReject
9	AdmissionRequest
10	AdmissionConfirm
11	AdmissionReject
12	BandwidthRequest
13	BandwidthConfirm
14	BandwidthReject
15	DisengageRequest
16	DisengageConfirm
17	DisengageReject
18	LocationRequest
19	LocationConfirm
20	LocationReject
21	InfoRequest
22	InfoRequestResponse
23	NonStandardMessage
24	UnknownMessageResponse
25	RequestInProgress

Table 10.45 Unknown Gatekeeper Messages *(continued)*

ID	Message
26	ResourcesAvailableIndicate
27	ResourcesAvailableConfirm
28	InfoRequestAck
29	InfoRequestNak
30	ServiceControlIndication
31	ServiceControlResponse

10.4.3.5 ENUM OUTPUT

This output is assigned to group `i` and occurs with Layer2 and Layer3 traces:

```
i[<controller>]: enum_query cr <CR> ch <CH>: <num> -> <length> <<answer pattern>>
```

Table 10.46 ENUM Output

Trace Output	Description
<cr>	Call reference.
<ch>	Media channel.
<num>	Phone number converted into ENUM domain format.
<length>	Length of the answer field in the DNS response in bytes. `0` appears if the number was not found.
<answer pattern>	Displays the DNS response. `0` appears if the number was not found.

10.4.3.6 EXAMPLES

The following examples are offline traces. You can generate them using the GATE Manager or FTP commands. The filename is trace.log. The following cases appear in the examples:

- Incoming H323 Call with FastStart ⇨
- Outgoing H323 Call with FastStart ⇨
- Fax Call ⇨

Incoming H323 Call with FastStart

```
[15:25:13.65] i[02]: h225accept from 172.16.0.200 s 4
[15:25:13.75] y[02]: h225rcv tpkt msg 5 h225cr 8006 addr 172.16.0.200 pt 0
[15:25:13.75] y[02]: h225 decode rc 0, q931 msg 5 (0), len 364
[15:25:13.75] y[02]: h225rcv setup voipcfg addr 172.16.0.200 rc 0 <DF> compr EABG
[15:25:13.75] y[02]: h225rcv faststart <A1B1E1G0>
[15:25:13.75] y[02]: h225rcv setup oad 01 00 <111> <> dad 01 <123456> rad <> bc 038090a3 0101
[15:25:13.75] y[02]: h225rcv setup h225cr 8006 FS:1(E,172.16.0.200,29000) TUNN:1 H245:0(0,0)
[15:25:13.75] y[02]: h225rcv setup h225cr 8006 cr 7
[15:25:13.75] i[02]: pstnsnd setup dad 123456 oad 1 cr 7 s 4
[15:25:13.75] s[00]: 00 01 52 4c 08 02 00 08 05 04 03 80 90 a3 18 03 a1 83 87 6c 04 81 31 31 31 70 07 81
31 32 33 34 35 36 7d 02 91 81
[15:25:13.75] i[02]: pstnrcv connresp cr 7 acc 5 ch 1
[15:25:13.75] x[02]: h225snd callproc typ d cr 7 pri 0
[15:25:13.75] r[00]: 00 01 01 54
[15:25:13.75] r[00]: 02 01 4c 54 08 02 80 08 0d 18 03 a9 83 87
[15:25:13.75] s[00]: 02 01 01 4e
[15:25:14.33] r[00]: 02 01 4e 54 08 02 80 08 01
[15:25:14.33] s[00]: 02 01 01 50
[15:25:14.33] i[02]: pstnrcv alert cr 7 cls ff
[15:25:14.33] i[02]: rtp start cr 7 ch 1 li 1 ri 1 st 2 fx 0 cp E txm 1
[15:25:14.33] x[02]: h225snd callproc typ 1 cr 7 pri 8
[15:25:14.34] a[02]: vp start(201) ch=0 local=29000 remote=ac1000c8:29000 agg=0 pcm=0
[15:25:14.38] a[02]: vp rtcp 0: RR Tx pc 0 oc 0 ji -1 rt 0 fl -1 cl -1
[15:25:14.38] a[02]: vp ch 0: in 0 out 74
[15:25:15.57] r[00]: 02 01 50 54 08 02 80 08 07 29 05 06 03 18 0f 17 4c 06 01 81 31 37 33 31
[15:25:15.57] s[00]: 00 01 54 52 08 02 00 08 0f
[15:25:15.57] i[02]: pstnrcv connresp cr 7 acc 10 ch 255
[15:25:15.57] x[02]: h225snd callproc typ 7 cr 7 pri 0
[15:25:15.58] r[00]: 00 01 01 56
[15:25:17.01] a[02]: vp rtcp 0: SR Rx pc 110 oc 1816 ji 158 rt -1 fl 2 cl 1
[15:25:20.09] a[02]: vp rtcp 0: SR Tx pc 277 oc 5496 ji 164 rt 0 fl 0 cl 0
[15:25:20.09] a[02]: vp ch 0: in 18166 out 20646
[15:25:20.09] a[02]: vp rtcp 0: SR Rx pc 258 oc 4634 ji 208 rt -1 fl 0 cl 1
[15:25:23.32] a[02]: vp rtcp 0: SR Tx pc 441 oc 8776 ji 176 rt 0 fl 0 cl 0
[15:25:23.32] a[02]: vp ch 0: in 28966 out 32900
[15:25:24.68] y[02]: h225rcv tpkt msg 5a h225cr 8006 addr 172.16.0.200 pt 800e7800
[15:25:24.68] y[02]: h225 decode rc 0, q931 msg 5a (5), len 33
[15:25:24.68] y[02]: h225rcv relack h225cr 8006 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[15:25:24.68] y[02]: h225rcv relack h225cr 8006 cau 0x10
[15:25:24.68] i[02]: rtp hold cr 7 ch 1
[15:25:24.68] s[00]: 00 01 56 52 08 02 00 08 45 08 02 80 90
[15:25:24.68] i[02]: h225 connection 4 terminated
[15:25:24.69] r[00]: 00 01 01 58
[15:25:25.89] r[00]: 02 01 52 58 08 02 80 08 4d
[15:25:25.89] s[00]: 00 01 58 54 08 02 00 08 5a
[15:25:25.94] i[02]: pstnrcv terminate connection (3201) cr 7 cau 1 err 16 state 17 ch 1 rsid 1
[15:25:25.94] i[02]: rtp stop cr 7 ch 1
[15:25:25.94] r[00]: 00 01 01 5a
[15:25:25.94] a[02]: vp ch 0: in 34096 out 38154
[15:25:25.94] a[02]: vp stop ch=0
```

Outgoing H323 Call with FastStart

```
[15:04:09.12] r[00]: 02 01 46 48 08 02 22 54 05 04 03 80 90 a3 18 03 a9 83 94 6c 06 01 81 31 31 31 31 70
04 81 33 32 31 7d 02 91 81
[15:04:09.12] s[00]: 02 01 01 48
[15:04:09.12] s[00]: 00 01 48 48 08 02 a2 54 0d 18 03 a9 83 94
[15:04:09.12] i[02]: pstnrcv setup dad DF:321 oad 1111 cc 0 id 15d006
[15:04:09.12] i[02]: pstnrcv get_voipcfg <DF>
[15:04:09.12] i[02]: h225connect to 172.16.0.200 cr 6
[15:04:09.12] x[02]: h225snd setup dad 1 cr 6
[15:04:09.12] r[00]: 00 01 01 4a
[15:04:09.15] y[02]: h225rcv tpkt msg d h225cr 6 addr 172.16.0.200 pt 80412800
[15:04:09.15] y[02]: h225 decode rc 0, q931 msg d (11), len 32
[15:04:09.15] y[02]: h225rcv msg d (11) h225cr 6 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[15:04:09.50] y[02]: h225rcv tpkt msg 1 h225cr 6 addr 172.16.0.200 pt 80412800
[15:04:09.50] y[02]: h225 decode rc 0, q931 msg 1 (3), len 121
[15:04:09.50] y[02]: h225rcv faststart <E1>
[15:04:09.50] y[02]: h225rcv alert h225cr 6 FS:1(E,172.16.0.200,29000) TUNN:1 H245:0(0,0)
[15:04:09.50] i[02]: rtp start cr 6 ch 1 li 1 ri 1 st 2 fx 0 cp E txm 1
[15:04:09.50] s[00]: 00 01 4a 48 08 02 a2 54 01 1e 02 80 88
[15:04:09.50] a[02]: vp start(201) ch=0 local=29000 remote=ac1000c8:29000 agg=0 pcm=0
[15:04:09.50] r[00]: 00 01 01 4c
[15:04:09.53] a[02]: vp rtcp 0: RR Tx pc 0 oc 0 ji -1 rt 0 fl -1 cl -1
[15:04:09.53] a[02]: vp ch 0: in 0 out 74
[15:04:11.79] y[02]: h225rcv tpkt msg 7 h225cr 6 addr 172.16.0.200 pt 80412800
[15:04:11.79] y[02]: h225 decode rc 0, q931 msg 7 (2), len 79
[15:04:11.79] y[02]: h225rcv connect h225cr 6 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[15:04:11.79] i[02]: pstnsnd connect cr 6
[15:04:11.79] s[00]: 00 01 4c 48 08 02 a2 54 07
[15:04:11.80] r[00]: 02 01 48 4e 08 02 22 54 0f
[15:04:11.80] s[00]: 02 01 01 4a
[15:04:12.50] a[02]: vp rtcp 0: SR Rx pc 21 oc 394 ji 201 rt -1 fl 0 cl 0
[15:04:16.13] a[02]: vp rtcp 0: SR Tx pc 192 oc 3236 ji 196 rt 0 fl 0 cl 0
[15:04:16.13] a[02]: vp ch 0: in 14612 out 13796
[15:04:17.98] y[02]: h225rcv tpkt msg 5a h225cr 6 addr 172.16.0.200 pt 80412800
[15:04:17.98] y[02]: h225 decode rc 0, q931 msg 5a (5), len 33
[15:04:17.98] y[02]: h225rcv relack h225cr 6 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[15:04:17.98] y[02]: h225rcv relack h225cr 6 cau 0x10
[15:04:17.98] i[02]: rtp hold cr 6 ch 1
[15:04:17.98] s[00]: 00 01 4e 4a 08 02 a2 54 45 08 02 80 90
[15:04:17.98] i[02]: h225 connection 4 terminated
[15:04:17.99] r[00]: 00 01 01 50
[15:04:18.04] r[00]: 02 01 4a 50 08 02 22 54 4d 08 02 84 90
[15:04:18.04] s[00]: 00 01 50 4c 08 02 a2 54 5a
[15:04:18.06] i[02]: pstnrcv terminate connection (3201) cr 6 cau 90 err 16 state 17 ch 1 rsid 1
[15:04:18.06] i[02]: rtp stop cr 6 ch 1
[15:04:18.06] r[00]: 00 01 01 52
[15:04:18.06] a[02]: vp ch 0: in 21288 out 20708
[15:04:18.06] a[02]: vp stop ch=0
```

Fax Call

```
[16:00:40.44] i[02]: h225accept from 172.20.0.200 s 4
[16:00:40.49] y[02]: h225rcv tpkt msg 5 h225cr 8007 addr 172.20.0.200 pt 0
[16:00:40.49] y[02]: h225 decode rc 0, q931 msg 5 (0), len 251
[16:00:40.49] y[02]: h225rcv setup voipcfg addr 172.20.0.200 rc 0 <DF> compr EABG
[16:00:40.49] y[02]: h225rcv faststart <E0G0>
[16:00:40.49] y[02]: h225rcv setup oad 00 00 <> <> dad 01 <123456> rad <> bc 038090a3 0101
[16:00:40.49] y[02]: h225rcv setup h225cr 8007 FS:1(E,172.20.0.200,29000) TUNN:1 H245:0(0,0)
[16:00:40.49] y[02]: h225rcv setup h225cr 8007 cr 14
[16:00:40.49] i[02]: pstnsnd setup dad 123456 oad  cr 14 s 4
[16:00:40.49] s[00]: 00 01 5a 54 08 02 00 09 05 04 03 80 90 a3 18 03 a1 83 88 70 07 81 31 32 33 34 35 36
7d 02 91 81
[16:00:40.49] i[02]: pstnrcv connresp cr 14 acc 5 ch 1
[16:00:40.49] x[02]: h225snd callproc typ d cr 14 pri 0
[16:00:40.50] r[00]: 02 01 54 5c 08 02 80 09 0d 18 03 a9 83 88
[16:00:40.67] r[00]: 02 01 56 5c 08 02 80 09 01
[16:00:40.67] i[02]: pstnrcv alert cr 14 cls ff
[16:00:40.67] i[02]: rtp start cr 14 ch 1 li 1 ri 1 st 2 fx 0 cp E txm 2
[16:00:40.67] x[02]: h225snd callproc typ 1 cr 14 pri 8
[16:00:40.70] a[02]: vp start(201) ch=0 local=29000 remote=ac1000c8:29000 agg=0 pcm=0
[16:00:40.74] a[02]: vp rtcp 0: RR Tx pc 0 oc 0 ji -1 rt 0 fl -1 cl -1
[16:00:40.74] a[02]: vp ch 0: in 0 out 74
[16:00:40.90] r[00]: 02 01 58 5c 08 02 80 09 07 29 05 06 03 18 0f 3b 4c 08 01 81 31 32 33 34 35 36
[16:00:40.90] s[00]: 00 01 5c 5a 08 02 00 09 0f
[16:00:40.90] i[02]: pstnrcv connresp cr 14 acc 10 ch 255
[16:00:40.90] x[02]: h225snd callproc typ 7 cr 14 pri 0
[16:00:41.98] a[02]: vp rtcp 0: SR Rx pc 134 oc 1340 ji 195 rt -1 fl 0 cl 0
[16:00:43.29] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.29] y[02]: h225 decode rc 0, q931 msg 62 (6), len 123
[16:00:43.29] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.29] i[02]: h245rcv(1) cr 14 TerminalCapabilitySet peer=<EG> cfg=<EABG>
[16:00:43.29] i[02]: h245snd(1) cr 14 TerminalCapabilitySetAck
[16:00:43.29] i[02]: h245snd(1) cr 14 TerminalCapabilitySet <EABG>
[16:00:43.51] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.51] y[02]: h225 decode rc 0, q931 msg 62 (6), len 63
[16:00:43.51] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.51] i[02]: h245rcv(1) cr 14 TerminalCapabilitySetAck
[16:00:43.72] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.72] y[02]: h225 decode rc 0, q931 msg 62 (6), len 74
[16:00:43.72] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.72] i[02]: h245rcv(1) cr 14 RequestMode t38=1
[16:00:43.72] i[02]: h245snd(1) cr 14 RequestModeAck
[16:00:43.73] i[02]: h245snd(1) cr 14 CloseLogicalChannel cn=1
[16:00:43.73] i[02]: h245snd(1) cr 14 OpenLogicalChannel cn=1 cpr=G sessid=1 ctrl=172.20.0.100:29001
[16:00:43.73] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.73] y[02]: h225 decode rc 0, q931 msg 62 (6), len 68
[16:00:43.73] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.73] i[02]: h245rcv(1) cr 14 CloseLogicalChannel cn=1 (1)
[16:00:43.73] i[02]: h245snd(1) cr 14 CloseLogicalChannelAck cn=1
[16:00:43.73] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.73] y[02]: h225 decode rc 0, q931 msg 62 (6), len 92
[16:00:43.73] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.73] i[02]: h245rcv(1) cr 14 OpenLogicalChannel cn=1 cpr=G sessid=1 ctrl=172.20.0.200:29001
[16:00:43.73] i[02]: h245snd(1) cr 14 OpenLogicalChannelAck cn=1 sessid=1 media=172.20.0.100:29000
[16:00:43.73] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.73] y[02]: h225 decode rc 0, q931 msg 62 (6), len 64
[16:00:43.73] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.73] i[02]: h245rcv(1) cr 14 CloseLogicalChannelAck cn=1
[16:00:43.73] y[02]: h225rcv tpkt msg 62 h225cr 8007 addr 172.20.0.200 pt 80410800
[16:00:43.73] y[02]: h225 decode rc 0, q931 msg 62 (6), len 83
[16:00:43.73] y[02]: h225rcv facility h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:00:43.73] i[02]: h245rcv(1) cr 14 OpenLogicalChannelAck cn=1 sessid=1 media=172.20.0.200:29000
```

```
[16:00:43.73] i[02]: rtp start cr 14 ch 1 li 1 ri 1 st 3 fx 0 cp G txm 2
[16:00:43.73] i[02]: rtp start cr 14 ch 1 li 1 ri 1 st 3 fx 1 cp G txm 2
[16:00:43.74] a[02]: vp start2 ch=0 remote=ac1000c8:29000
[16:00:43.74] a[02]: vp start(401) ch=0 local=29000 remote=ac1000c8:29000 agg=0 pcm=0
[16:00:47.70] a[02]: vp rtcp 0: SR Tx pc 13 oc 352 ji 132 rt 0 fl 0 cl 0
[16:00:53.63] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:00:59.14] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:02.12] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:07.16] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:11.82] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:18.06] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:21.15] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:26.10] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:28.89] a[02]: vp rtcp 0: RR Tx pc 13 oc 352 ji -1 rt 0 fl -1 cl -1
[16:01:33.14] y[02]: h225rcv tpkt msg 5a h225cr 8007 addr 172.20.0.200 pt 80410800
[16:01:33.14] y[02]: h225 decode rc 0, q931 msg 5a (5), len 33
[16:01:33.14] y[02]: h225rcv relack h225cr 8007 FS:0(-,0,0) TUNN:1 H245:0(0,0)
[16:01:33.14] y[02]: h225rcv relack h225cr 8007 cau 0x10
[16:01:33.14] i[02]: rtp hold cr 14 ch 1
[16:01:33.15] s[00]: 00 01 5e 5a 08 02 00 09 45 08 02 80 90
[16:01:33.15] i[02]: h225 connection 4 terminated
[16:01:33.19] r[00]: 02 01 5a 60 08 02 80 09 4d
[16:01:33.19] s[00]: 00 01 60 5c 08 02 00 09 5a
[16:01:33.19] i[02]: pstnrcv terminate connection (3201) cr 14 cau 1 err 16 state 17 ch 1 rsid 1
[16:01:33.19] i[02]: rtp stop cr 14 ch 1
[16:01:33.23] a[02]: vp ch 0: in 85542 out 4346
[16:01:33.23] a[02]: vp stop ch=0
```

10.4.4 REMOTE OUTPUT

This trace option provides output for communication with the GATE Manager or NMS. To activate this option, activate the section **Remote** in the GATE Manager. You can choose the depth of the trace output: **Error** is limited to error messages; **Debug** provides information; **Detail** provides the entire packet.

Output is defined with a g, and the port number is 99.

The following output shows an established GATE Manager connection:

```
g[99]:moip: accept rc=2 ipad=<ip address> port=<port>
```

Table 10.47 Remote Output

Trace Output	Description
<ip address>	Remote system's IP address with GATE Manager.
<port>	Origination port for the GATE Manager connection.

```
g[99]:moip: <direction> <length>
```

Table 10.48 Remote Output

Trace Output	Description
<direction>	recv Packets received from the remote system send Packets sent to the remote system write Output for communication with the internal remote interface read Output for communication from the internal remote interface
<length>	Data length in bytes.

All other trace output appears in detail mode in ASCII and are also translated.

10.4.5 SMTP TRACE OUTPUT

This trace option provides output for communication with the mail server that occurs when status information or files are sent, or in the other direction, which e-mails are received and converted to SMS or USSD.

To activate this option, activate the section **Mail** in the GATE Manager. You can choose the depth of the trace output: **Error** is limited to error messages; **Debug** provides information; **Detail** provides the entire packet.

Output is defined with a m, and the port number is 99.

Sending Files or Status Information

Global message output:

```
m[99]:mail: sendmail (<length>)
```

Table 10.49 SMTP Output: Sending Files or Status Info

Trace Output	Description
<length>	Data length in bytes.

Detailed message output:

```
m[99]:mail: sendmail: <Faccount> <ip address> <Taccount> <domain> <subject> <content>
```

Table 10.50 SMTP Output: Sending Files or Status Info

Trace Output	Description
<Faccount>	Sender's e-mail account (cdr, alarm, file, etc.).
<ip address>	SMTP server's IP address.
<Taccount>	Recipient's e-mail account.
<domain>	Recipient's domain.
<subject>	Content of the subject field; serial number of the sender system.
<content>	Content of the message's body.

All other trace output appears in detail mode in ASCII and are also translated.

Receiving E-Mail Messages and Sending Them as SMS or USSD

The following output displays communication of an incoming SMTP connection:

```
m[99]:mail: accept: ipad=<ip address> port=<port>
```

Table 10.51 SMTP Output: Receiving E-Mail and Sending as SMS or USSD

Trace Output	Description
<ip address>	The SMTP peer system's IP address.
<port>	The SMTP peer system's origination port.

The following output displays which packets are sent to the SMTP peer:

```
m[99]:mail: mysend <<content>>
```

Table 10.52 SMTP Output: Receiving E-Mail and Sending as SMS or USSD

Trace Output	Description
<content>	Content of the transmitted packet.

All other trace output appears in detail mode in ASCII and are also translated.

The following output displays which packets are received from the SMTP peer:

```
m[99]:mail: recv (<length>)
```

Table 10.53 SMTP Output: Receiving E-Mail and Sending as SMS or USSD

Trace Output	Description
<length>	Data length in bytes.

All other trace output appears in detail mode in ASCII and are also translated.

The following output shows that the SMTP connection is being closed:

```
m[99]:mail: terminate_session
```

The mail module now converts the e-mail message to the internal format and then sent as SMS or USSD. Bulk mail (several recipient entries for the same e-mail) appear as individual messages:

```
m[99]:mail: newMail2Host r=<Taccount> f=<Faccount> s=<subject> d=<content>
```

Table 10.54 SMTP Output: Receiving E-Mail and Sending as SMS or USSD

Trace Output	Description
<Faccount>	One entry from the sender’s To field.
<Taccount>	Content of the From field.
<subject>	Content of the subject field; usually not used.
<content>	Content of the message’s body; is sent as SMS or USSD.

The following output appears when the message has been successfully sent:

```
m[99]:mail: rcvmail <Faccount> -> <Taccount>, done
```

This is converted in the confirmation message, with the subject `sent`. The output in the subsequent communication with the mail server are identical to those described above in Sending Files or Status Information ⇨.

The following output appears when errors occur during transmission of the SMS or USSD message:

Message transmission was faulty and will be repeated:

```
m[99]:mail: rcvmail <Faccount> -> <Taccount>, failed, will retry (<num>)
```

Table 10.55 SMTP Output: Transmission Error

Trace Output	Description
<num>	Current number of retries.

Retried message transmission was also faulty, and an e-mail will be generated:

```
m[99]:mail: rcvmail <Faccount> -> <Taccount>, failed <num> times
```

The output in the subsequent communication with the mail server are identical to those described above in Sending Files or Status Information ⇨.

Receiving SMS or USSD and Sending as E-Mail

The following output shows the internal format when an SMS or USSD message is sent to the mail module. This output is generated when transmission of the SMS or USSD message was not possible:

```
m[99]:mail: DATA_IND (<length>)
```

All other trace output appears in detail mode in ASCII and are also translated. The output in the subsequent communication with the mail server are identical to those described above in Sending Files or Status Information ⇨.

10.4.6 NUMBER PORTABILITY TRACE OUTPUT

This trace option provides output for the communication with the iMNP database. To activate this option, activate the section **Number Portability** in the GATE Manager. Output is defined with an n, and the port number is 99.

The following output appears when the system sets up a TCP session with the iMNP is being set up:

```
n[99]:np: connecting to <ip addr>
```

Table 10.56 Number Portability Output: Connection with iMNP

Trace Output	Description
<ip address>	The iMNP system’s IP address.

The following output shows that the connection has been established:

```
n[99]:np: connect to <ip addr> ok
```

The following output shows that the connection attempt failed:

```
n[99]:np: connect to <ip addr> failed
```

The following output shows a keep alive packet from the iMNP to keep the TCP session open:

```
n[99]:np: recv <>
```

Response to a number portability request that results in the call's routing:

```
n[99]:np: recv <N<num>>
```

Table 10.57 Number Portability Output: Response

Trace Output	Description
<num>	Ported or unported number provided by the database.

10.4.7 DTMF TONE TRACE OUTPUT

Output about the setup of connections with the DTMF module and DTMF tone recognition are debugged. The output differentiates between the groups `err` and `inf`. Output is defined with a `d`, and the port number is that of the virtual DTMF controller:

The following output shows incoming call setup to the DTMF module:

```
d[<ctrl>]: dtmf: msg <call state>, unknown id <id>, from 14
```

Table 10.58 DTMF Output: Incoming Call Setup

Trace Output	Description
<ctrl>	The virual controller's running number.
<call state>	3101 Incoming setup 3201 Disconnect request
<id>	Call identification number.

The following output shows transmitted signaling messages depending on the call state:

```
d[<ctrl>]: dtmf <message type> <id> <call state> 0
```

Table 10.59 DTMF Output: Signaling Messages

Trace Output	Description
<message type>	Send_d_connect For setup acknowledge and connect. send_alert_ind For alert. send_disconnect For disconnect
<id>	Call identification number.
<call state>	3110 Incoming setup 3102 Disconnect request 3804 Alert 3202 Disconnect confirmation

The following output shows that the media channel has been designated for DTMF tone recognition:

```
d[<ctrl>]: dtmf send_alloc <b_chan id_unset> <ctrl>/<b chan>
```

Table 10.60 DTMF Output: Media Channel Designation

Trace Output	Description
<b chan>	Internal media channel used.
<b_chan id_unset>	Media channel identification (in unset state).

```
d[<ctrl>]: dtmf: msg <msg>, id <b_chan id>, from 1, id <id>/<b_chan id_unset>
```

Table 10.61 DTMF Output: Media Channel Designation

Trace Output	Description
<msg>	`502` Media channel confirmation
	`102` Connect confirmation
	`602` Media channel free confirmation

The following output shows the output for negotiated DTMF tones:

```
d[<ctrl>]: dtmf send_info_ind <id> <<dtmf tone>>
```

11 FEATURE PACKAGES

The iGATE feature packages are modular expansion applications that provide services in addition to those offered with the standard software. Feature packages can be activated separately or in combination with one another, so that you can design your system according to your own needs.

The following feature packages are available:

- Dial-In/Callback Services (cf. Chapter 11.2 on page 198 ⇨)
- Least Cost Routing (cf. Chapter 11.3 on page 202 ⇨)
- Online Traffic Monitor (cf. Chapter 11.4 on page 208 ⇨)
- SMS Gateway (cf. Chapter 11.5 on page 214 ⇨)
- SS7-Specific Settings (cf. Chapter 11.7 on page 221 ⇨)
- Ported Number Screening (cf. Chapter 11.6 on page 219 ⇨)

11.1 ACTIVATING THE LICENSE

Each feature package requires a license. Once you have ordered a feature package, you can activate the license:

The `/boot/` directory of each system contains a file called license.key, which contains information on the system's ID, the included components, which feature packages are active and the license number:

Example:

```
[IDENTIFICATION]
SYSTEM: TELES.iGATE
SERNO:  VT810011
AUTOR:  create   Wed Sep 09 15:01:09 2006

[COMPONENTS]
...
CARD99:11 d1 S0  PB900034
...

[FEATURES]
PRI:Max
SS7:0
GSM:Max
IP:Max
VoIP:Max
SIM manager: On
DDI and call back: Off
least cost routing: On
statistics and CDR: On
SMS gateway: On
ported number screening: Off
roaming: Off

[SIGNATURE]
00000000000license0number00000000000
```

You will receive a new license.key file any time you order a new license package. Simply save the new file, overwriting the old file, and restart the system.

Deleting or making changes in the `license.key` file will delete any feature package licenses, causing the system to revert to the standard configuration!

11.2 DLA/CALLBACK SERVER FUNCTIONALITY

This package contains money-saving features that expand the functionality of your iGATE to include callback capability and DTMF services. It is particularly useful for companies with employees who travel often, because it eliminates expensive roaming fees:

11.2.1 CALL CONNECTOR AND CALLBACK SERVER

Depending on your iGATE, various intelligent solutions as a call server are possible. The most important scenarios and properties are described here. The scenarios can also be combined to suit your needs.

- Special announcement
- DLA with DTMF
- DLA with fixed destination number
- Callback with DTMF for the second leg number (known OAD or fixed callback number)
- Callback with DTMF and OAD as callback number
- Callback with DTMF and pre-configured callback number
- Callback for a fixed second leg
- DLA with DTMF and PIN for the first leg and callback for the second leg
- Using a PIN in front of the call number
- Callback via SMS
- Callback via HTTP

Numbers transmitted using DTMF tones can be ended by entering a # sign. Otherwise, a 5-second timer is set, after which DTMF transmission will automatically end.

If the callback call is set up from the mobile network, the SIM must be available 24 hours a day. We recommend that you reserve a SIM for this service. Otherwise, another call could block the call initiating callback, which limits the effectiveness of the service.

CDR entries for calls routed as Callback with DTMF include the connection times for the A and B subscribers. The times are separated by a slash (`/`). If no connection is established to the B subscriber, an entry recording the A subscriber's connection time is generated in the `failed.log` file.

Activating DTMF Tone Recognition

The iGATE can recognize DTMF tones and initiate calls with these tones. In the pabx.cfg, enter a virtual DTMF controller, as described in Table 5.13 ➩. The corresponding Subscriber entry contains the options:

```
TRANSPARENT ROUTER CHMAX[5]
```

The `5` refers to the maximum number of simultaneous channels used for DTMF recognition.

Example:

```
...
Controller06 = 41 DTMF
...
Subscriber06 = TRANSPARENT ROUTER CHMAX[5]
...
```

The iGATE must be restarted to activate this configuration.

11.2.1.1 SPECIAL ANNOUNCEMENT

An announcement can be played immediately after the connection has been established. The announcement can be defined in the virtual DTMF controller's Subscriber line using the following entry:

In the `pabx.cfg` file:
`DTMF[<sec>,/<dir>/<file>]`

<sec> refers to the maximum number of seconds that may pass before the next DTMF tone is entered, <dir> refers to the directory, in which the announcement file is saved. boot or data are possible. The file extension must be 711.

The file's sound format must be PCM!

Example: In this example, a maximum of 5 channels can recognize DTMF tones and change them into dialing data. The announcement is named DTMF.711 and is saved in the boot directory:

```
Subscriber06 = TRANSPARENT ROUTER DTMF[30,/boot/DTMF.711] CHMAX[5]
```

11.2.1.2 DLA WITH DTMF

The user dials a number in the system that is connected with the DTMF platform. She then enters the number with which she would like to be connected.

Make the following entries in the route.cfg to connect a call directly:

```
MapAll<number>=<DTMFport>DTMF
MapAllDLA=<port>
```

Example: In the following example, the call from the number 123 is connected to the DTMF platform and the call that comes in as DTMF tones is directed to port 9:

```
MapAll123=41DTMF
MapAllDLA=9
```

11.2.1.3 DLA WITH FIXED DESTINATION NUMBER

The user dials a number in the system that is connected directly with a fixed external number (e.g. international subsidiary number). Make the following entry in the route.cfg:

```
MapAll<num>=<port><fixed num>
```

Example: In the following example, the call comes into the number 123456 and is connected to the number 004311111 at port 9.

```
MapAll123456=9004311111
```

11.2.1.4 CALLBACK WITH DTMF AND OAD AS CALLBACK NUMBER

The user calls a number that is defined so that the user will be called back based on his OAD. An alerting occurs. The user hangs up and is called back. After the user has taken the call, the destination number is entered using DTMF tones. When he has finished dialing, the connection to the destination number is established.

Callback is not possible for VoIP calls.

The following entries in route.cfg will initiate callback to the calling party’s number:

```
MapAllDTMF=<DTMFport>DTMF
MapAllDLA=<port>
MapAll<number>=CALLB
MapAllCB=<port>
```

Example: In this example, the call with the number 123 is connected with the OAD and the number that comes in as DTMF is directed to port 9:

```
MapAllDTMF=41DTMF
MapAllDLA=9
MapAll123=CALLB
MapAllCB=9
```

11.2.1.5 CALLBACK WITH DTMF AND PRE-CONFIGURED CALLBACK NUMBER

The user calls a predefined number that is mapped to a defined callback number. An alerting occurs. The user hangs up and is called back at a fixed number. After the user has accepted the call, she must enter the destination number via DTMF. The connection is set up when she finishes dialing.

Callback is not possible for VoIP calls.

Make the following entries in route.cfg to initiate callback to a fixed number:

```
MapAllDTMF=<DTMFport>DTMF
MapAllDLA=<port>
MapAll<number>=CALL<callbacknumber>
```

Example: In the following example, the call with the number 123 is connected with the number 03012345. The number that comes in as DTMF is directed to port 9:

```
MapAllDTMF=41DTMF
MAPAllDLA=9
MapAll123=CALL903012345
```

11.2.1.6 CALLBACK TO OAD AND FIXED SECOND LEG

The user calls a predefined number in the system. An alerting occurs. The user hangs up and is called back based on her OAD. After the user accepts the call, she is connected to a fixed, preconfigured number (e.g. operator or corporate central office.

Callback is not possible for VoIP calls.

Make the following entries in route.cfg:

```
MapAllDTMF=<port><num>
MapAll<num>=CALLB
MapAllCB=<port>
```

Example: In the following example, the caller dials 123456 and her OAD is called back through port 9. She is then connected with the operator's number 0 through port 10.

```
MapAllDTMF=100
MAPAll123456=CALLB
MapAllCB=9
```

11.2.1.7 DLA WITH DTMF AND PIN FOR FIRST LEG AND CALLBACK FOR SECOND LEG

The user dials a number in the system that is connected to the DTMF platform. He then enters a predefined PIN that maps him to a predefined fixed number that is to be called back. He then hangs up. After he takes the callback, he can enter the second leg number using DTMF tones.

Make the following entries in route.cfg:

```
MapAllDTMF=<DTMFport>DTMF
MapAll<num>=<DTMFport>DTMF VOICE
MapAllDLA<num>=CALL<num> VOICE
MapAllDLA=<port> VOICE
```

Example: The number 123456 is dialed and the PIN 123# is entered. The call is then connected to the number 004930123456. The destination number can now be transmitted through port 9 using DTMF tones:

```
MapAllDTMF=41DTMF
MAPAll123456=41DTMF VOICE
MapAllDLA123=CALL9004930123456 VOICE
MapAllDLA=9 VOICE
```

The user must enter a # following the PIN. Otherwise the callback to the predefined number will not occur.

11.2.1.8 USING A PIN IN FRONT OF THE CALL NUMBER

To prevent abuse, the following entry can be made to configure a PIN in front of the actual call number:

```
MapAllDLA=$PIN
MapAllPIN<pin>=<port>
```

Example: In the following example, the DTMF tones are analyzed, whereby the first 4 (1111) corresponds with the PIN. The call to subscriber B is initiated when the PIN has been entered correctly. All other DTMF tones are directed to port 9:

```
MapAllDLA=$PIN
MapAllPIN1111=9
```

11.3 LEAST COST ROUTING

iGATEs are connected between the customer’s private branch exchange (PBX) and the public telephone network (ISDN) and/or VoIP. The customer saves connection charges and can effortlessly and automatically connect to the corporate network as needed using one of six routing methods:

- Carrier selection
- Dedicated lines
- Direct line access with subaddressing
- Direct line access with DTMF
- Callback with subaddressing
- Callback with DTMF

This manual contains information only on carrier selection. If you would like to configure any other variation, please contact TELES or refer to the TELES Infrastructure Systems Manual Version 4.5, Chapter 3.

Calls are routed transparently for the PBX and its users. iGATEs can generate charges and route calls using alternate settings in case of network failures. The provider can access the system via ISDN for routine maintenance and monitoring.

The following additional services are supported by this feature package:

- Generation of charges
- Time-controlled configuration
- Alternative routing

11.3.1 CARRIER SELECTION

Carrier selection is currently one of the most commonly used routing methods supported by the iGATE. In the iGATE, this routing process also includes direct calls into the mobile network or through a VoIP network. That means the system is a full-fledged second generation LCR.

11.3.1.1 ROUTING ENTRIES

Use the MapAll command to route calls using Carrier Selection.

a) Use the following syntax for connections routed via the provider:
`MapAll<AreaCode>=9<CarrierSelection><AreaCode>`
where <AreaCode> is the number or number range to be routed and <CarrierSelection> is the access number required to reach the provider's network.

b) For unrouted connections (placed via the public telephone network), use:
`MapAll<AreaCode>=9<AreaCode>`

c) To block undesired carrier selection prefixes use:
`MapAll<CarrierSelection>=&91;(Busy signal)`

In the following example, calls to international destinations are terminated through the VoIP interface. The profile names iG1 and iG2 in the routing entries refer to different VoIP carriers. Calls to the mobile network (01555 and 01556) are routed directly through SIM cards for the corresponding mobile carriers (LAIN 26212 and 26213). All other national long distance and local calls are routed through an alternative carrier (01019). All calls from the PSTN to the PBX are put through transparently.

Example:

```
MapAll001=40iG1:001
MapAll0044=40iG2:0044
...
MapAll01555=2621201555
MapAll01556=2621301556
...
MapAll01=90101901
MapAll02=90101902
...
MapAll09=90101909

MapAll1=9010191
MapAll2=9010192
...
MapAll9=9010199

Restrict9=10
```

Be sure to enter phone numbers in the routing file in ascending order.

11.3.2 ALTERNATIVE ROUTING SETTINGS

Alternative routing refers to the ability to establish connections using a different (alternative) network in case of provider failure (e.g. all mobile controllers are in use). Alternative routing ensures uninterrupted operation of the attached PBX. In such cases, connections are often made via the public network using the Redirect command:

```
MapAll<num>=<port><num>
Redirect3<port><num>=<placeholder>
MapAll<placeholder>=<alt port><num>
```

Example:

```
MapAll01555=2621201555
Redirect32621201555=A
MapAllA=901555
```

11.3.3 CHARGE MODELS

iGATEs can either generate charge information or transmit received charges from the public or corporate networks to the attached PBX. Charge simulation is achieved using variables, which ensure a great degree of flexibility for the implementation of many different charge models including:

- Charge units per time unit
- Flat rate (initial charge without time interval)
- Initial charge plus time interval
- Initial charge plus time interval after delay
- Time interval and/or flat rate plus received charges
- Received charges only or no charge information
- Initial toll-free period with retroactive charge generation afterwards
- Price-per-minute (with whole second accuracy)

In this chapter, **unit** means that charge information is transmitted as a whole-numbered value, and **currency** means that the charge information is sent as a currency amount (e.g. EUR 3.45). The charge impulse generation options can be set for each mapping by adding charge-specific arguments to the MapAll commands as shown below. The use of each variable is explained in Table 11.1 ⇨.

`MapAllsrc=dst mode time start/wait` and

`MapCallBackOutprovsrc=dst mode time start/wait`.

Table 11.1 Charge Variables

Variable	Purpose
time	Determines the length of each time interval (how long each unit lasts). The value is entered in seconds and hundredths or thousandths of a second (the maximum value accepted is 655.35 seconds, 65.535 if thousandths are entered). If time is set to zero or not present no charges are generated, external charge information is passed through if received.
start	Sets the initial unit level. Enter a value between 0 and 127 whole units. If you want to use a flat rate, set the desired number of units here and set the wait to 255 to turn off the time interval.
wait	Determines the delay after which charge generation begins. Once this time has elapsed, charge impulses are sent in the interval determined with time. Enter a value between 0 and 254 seconds. 255 deactivates the charge pulse. In this case, the time variable is ignored.

Any external charges can be added to the generated charges by adding 128 to the *start* value. (The value range for the initial unit level is still set from 0 to 127). The maximum supported number of units per connection is 32767 units.

Additional adjustments may be made to allow for the implementation of new charge models.

- When charge information is sent as Currency, values can be expressed in thousandths for greater precision in charge calculation.

  For the internal Layer 3 protocols, charges can be specified to the third decimal place (thousandth) using the /Value option (Example: /Value:1.056). In this fashion, charges can be generated for units of currency requiring accuracy to the third decimal place or for fractions such as tenths of a cent. This allows for greater flexibility in the transmission of charges to terminal devices. In order to make use of this option, connected devices must support "AOC-D Currency". In the current version, this option is only available for the DSS1 protocol.
- A multiplication factor can be specified for received or generated charges.

  During the charge generation process, each charge unit is multiplied by a preset factor. This factor appears in the mapping entry after the time and start/wait variables (MapAllsrc=dst mode time start/wait*factor). Each unit, for example, can be converted to 12 cents. The following example illustrates the use of this feature:

Example: In the following example, all received charge units are multiplied by 12 and passed on. If AOC-Currency is set on the internal port, each unit appears as 12 cents.
The multiplication factor is also used to implement two new charge models:

- – If the factor value exceeds 128, this marks the use of an initial toll-free phase followed by retroactive charge generation.
- – If the multiplication factor is set to 255, a "minute price" is used in place of the time variable.

```
...
MapAll1=91 1 128/255*12
...
```

These charge models are explained on page 206 ⇨.

11.3.4 GENERATING CHARGES WITH THE IGATE

To generate charges for the attached PBX, add the charge variables described in Table 11.1 ⇨ to the MapAll commands according to the necessities of the corporate network environment.

Example 1 In the following mapping example, time=1.65, start=131, wait=0. Three initial tariff units (131-128) are transmitted upon connection and a new unit is generated every 1.65 seconds and transmitted the next full second. Charges received from the public network for the connection to the corporate network dial-in node are added and transmitted (because 128 has been added to the start variable's value).

```
...
MapAll0172=9123450172 1.65 131/0
...
```

Example 2 Upon connection establishment, 3 initial tariff units (131-128) are transmitted. Then a 10-second delay (wait=10) elapses before charge impulses are generated according to the time variable (a new unit is generated every 1.65 seconds and transmitted the next full second). Charges received from the public network for the connection to the corporate network dial-in node are added and transmitted (because 128 has been added to the start variable's value).

```
...
MapAll0172=9123450172 1.65 131/10
...
```

New charge models can be implemented by taking advantage of the multiplication factor in conjunction with the *time* and *start/wait* variables.

Retroactive charge generation after initial toll-free period

Example: The charge generation process has been expanded to allow for the implementation of this new charge model. In this scenario, an initial period is free of charge, but after this period charges are calculated for the entire call. For example: the first minute is free, but as soon as the second minute begins, charges are incurred for the first minute as well.
The multiplication factor is set to a base value of 128. If the value exceeds this base, the remaining value represents the number of units charged with each *time* interval. The following configuration generates one unit (129-128) per minute (*time*=60 seconds) retroactively after the first minute (*wait*=60 sec.):

```
...
MapAll030=901019030 60 0/60*129
...
```

"Price per minute"

A price per minute charge model can be implemented as of version 5.01 in one of two ways:

- either the attached PBX supports Advice of Charges as Currency
- or if not, the PBX can be configured to assign one thousandth (1⁄1000) of a currency unit (€0.001 or 1⁄10 of a cent) to each charge unit.

If thousandths are defined, a maximum value of 65.535 is possible. If tenths are defined, a maximum value of 6553.5 is possible.

This model does not always guarantee whole second accuracy (depending on the rates), but it is significantly more precise than the standard charge generation method.

Example 1 If the attached PBX supports Advice of Charges as Currency, include the following line in the iGATE's pabx.cfg:

```
...
Controller01=10 NTS2M DSS1 CRC4 UNIT:€ VALUE:0.001
...
```

Example 2 If the PBX does not support this AOC model, but allows for the assignment of one thousandth (1⁄1000) of a currency unit (€0.001 or 1⁄10 of a cent) for each charge unit, the above entry need not be present. The configuration entries must make use of the multiplication factor for a single unit as shown below:

```
...
MapAll902=90103002 1.00 0/0*4 ; each second costs €0.004 (€0.24 / minute)
MapAll909=90108809 1.00 0/0*5 ; each second costs €0.005 (€0.30 / minute)
...
```

Example 3 If the minute price does not allow generated charges to "fit" evenly into a second (such as 20 cents per minute or 0.33 cents per second), the system can be configured to generate 10 "points" every 3 seconds (€0.01 or 1 cent):

```
...
MapAll902=90101302 3.00 0/0*10 ; 3 seconds cost €0.01 (€0.20 / minute)
MapAll909=90105009 2.00 0/0*3  ; 2 seconds cost €0.003 (€0.09 / minute)
...
```

Example 4 The "points" method allows for a more precise calculation of smaller intervals.
The price per minute can also be explicitly specified in each routing entry by setting the multiplication factor to 255, to signalize to the system that a minute price is being used instead of the interval usually specified with the time variable. The attached PBX must support Advice of Charges as Currency, and the appropriate settings must be made in the iGATE's pabx.cfg as described on page 207 ⇨. The examples below show sample entries with rates of 18 and 9 cents per minute:

```
...
MapAll902=90101302 0.18 0/0*255 ; €0.18 / minute
MapAll909=90105009 0.09 0/0*255 ; €0.09 / minute
...
```

and

```
...
Controller01=10 NTS2M DSS1 CRC4 UNIT:€ VALUE:0.010
...
```

Example 5 If greater precision is desired (1/1000 of a currency unit – $0.001 or 1/10 of a cent), use settings such as the following:

```
...
MapAll902=90101302 1.80 0/0*255 ; €0.18 / minute
MapAll909=90105009 0.90 0/0*255 ; €0.09 / minute
...
```

and

```
...
Controller01=10 NTS2M DSS1 CRC4 UNIT:€ VALUE:0.001
...
```

11.4 ONLINE TRAFFIC MONITOR

The Online Traffic Monitor allows you to collect and monitor statistics and call detail records (CDRs). The following functions are possible with this feature package:

- ASR calculation
- Generation of CDRs
- Generation of online CDRs using e-mail

11.4.1 ASR CALCULATION AND RESETTING STATISTIC VALUES

When this function is configured in the pabx.cfg file, statistical values, such as the number of minutes, number of calls, ASR (Answer Seizure Ratio), etc., are calculated for the entire system at a defined time. These statistics are then copied into a specified file and reset at 0.

This information can also be sent to an e-mail or SMS recipient. The following syntax must be used:

```
StatisticTime=/data/asr.log <hh:mm> <day> @<account>
```

ASR2 is the ratio of connected calls to total calls, and ASR1 is the ratio of total calls to connected calls disconnected by the A party. ASR1 values are intended to provide you with an idea of the availability of the mobile network.

Example: In the following example, the system's statistic values are saved daily into the file `asr.log` and sent to an e-mail account.

```
StatisticTime=/data/asr.log 00:00 11111111 @<account>
```

Example: In the following example, the system's statistic values are saved monthly into the file `asr.log` and sent to an SMS recipient.

```
StatisticTime=/data/asr.log 00:00 01. @SMS<mobile number>
```

Example: If ?? appears instead of a specified hour, the ASR is written into the asr.log file once every hour. The values are reset to zero in the twenty-third hour:

```
StatisticTimeReset=/data/asr.log ??:00
```

Example: The next example shows how the statistics appear in the file into which they are copied. The following information is listed in the following order: day and time of the entry, followed by the system name. Calls: connected calls followed by the total number of calls in parentheses. The total number of minutes terminated by the system, followed by the ASR1 value, the external ASR for the traffic source (ext) and the internal ASR for the iGATE (int). These values can differ if a significant number of calls cannot be routed through the iGATE or an insufficient number of channels is available for a prefix. Finally, the average call duration (ACD) appears in the entry:

```
26.10.04-00:00:00,iGATE810000: Calls: 19351 (29716) - Minutes: 46647 - ASR1: 65.12% -  ASR(ext): 65.12% -
ASR(int): 65.30% - ACD: 144.63s
```

StatisticTimeReset=/data/asr.log <hh:mm> <day> performs the same function as the StatisticTime parameter, but also resets the counters (A-F).

Example: In the following example, the system's statistic values are saved on the 15th of every month into the file asr.log.

```
StatisticTimeReset=/data/asr.log 00:00 15.
```

It is not possible to configure both StatisticTimeReset and StatisticTime.
ASR values reset to 0 when the SIM card is changed using the GATE Manager.

11.4.2 GENERATING AND RETRIEVING CDRS

With the `Log` and `RrufLog` commands, you save CDRs and unconnected calls in the iGATE.

For these parameters (`Log` and `RrufLog`), a folder and file name must always be specified after the equal sign. The function is not active (no data is recorded) until a file name is specified.

Example:

```
Log=/data/cdr.log
RRufLog=/data/failed.log
```

With recording of files, system maintenance increases. You have to be sure to download or delete files and ensure that there is enough disk space left on the hard drive.

The service indicator listed in the call log and missed calls list describes the type of connection as a four digit hexadecimal number. The coding is conducted according to the 1TR6 standard. A few frequently used values are listed below:

0101	ISDN-telephony 3.1 kHz
0102	analog telephony
0103	ISDN-telephony 7 kHz
0200	Fax group 2
0202	Fax group 3
0203	Data via modem
0400	Telefax group 4
0500	SMS or BTX (64 kbps)
0700	Data transfer 64 kbps
07...	Bit rate adaptation
1001	Video telephone – audio 3.1 kHz
1002	Video telephone – audio 7 kHz
1003	Video telephone – video

For detailed information on how to automatically divide the files (e.g. on a daily basis), please refer to the Chapter 5.2.1.2 ➪.

11.4.2.1 CALL LOG

The following entry in the pabx.cfg configuration file activates the capability to generate CDRs in the iGATE:

```
Log=/data/cdr.log
```

The cdr.log file is stored in the data directory. New entries are always added to the end of the file. The file is open only during editing.

Each line represents an outgoing call:

DD.MM.YY-hh:mm:ss[Start],DD.MM.YY-hh:mm:ss[End],src,dst,service,dur,cause,charge_publine,[charge_sys]

DD – Day	hh – Hour	src – source/extension	dur – duration
MM – Month	mm – Minute	dst – destination	cause – reason for teardown
YY – Year	ss – Seconds	service – service indicator	charge_publine – from the public line
			charge_sys – generated by the system

The charge is specified in units. The service indicator listed will be one of the values shown on page 210 ➪. The example below shows a sample log file.

```
28.01.05-19:38:51,28.01.05-19:44:51,10611,9010193333333,0101,360,90,10
28.01.05-19:43:55,28.01.05-19:44:55,10610,26212015551111111,0101,60,90,3
28.01.05-19:32:54,28.01.05-19:44:55,10612,40iG2:004498989898,0101,721,90,15
28.01.05-19:41:34,28.01.05-19:45:34,10616,9010190123456,0101,240,90,4
28.01.05-19:44:19,28.01.05-19:45:49,10615,26212015553333333,0101,90,90,5
28.01.05-19:44:58,28.01.05-19:45:58,10610,26213015562222222,0101,60,90,3
28.01.05-19:46:01,28.01.05-19:47:12,10610,9010194444444,0101,71,90,5
28.01.05-19:46:18,28.01.05-19:47:48,10615,40iG1:00123232323232323,0101,90,90,4
28.01.05-19:47:03,28.01.05-19:48:07,10610,9010195555555,0101,64,90,4
28.01.05-19:48:07,28.01.05-19:49:07,10610,90101903066666666,0101,60,90,3
```

To differentiate between ports with the same number in the CDRs, a specific node number must be defined. You can expand the subscriber configuration line with the keyword NODE[<no.>] for this purpose. <no.> can be a string of between 1 and 15 characters:

`Subscriber<xx>=... NODE[<num>]`

Example:

```
29.08.05-09:45:24,29.08.05-09:46:33,923456789,[0007:01]01771111111,0101,69,0
```

In the above formula, <num> consists of a four-digit number that is included in the CDR.

Example: The following example shows the pabx.cfg configuration file changed according to the formula:

```
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NEXT NODE[0001]
Subscriber01=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0002]
Subscriber02=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0003]
Subscriber03=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0004]
Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0005]
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0006]
Subscriber06=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0007]
Subscriber07=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0008]
Subscriber08=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0009]
Subscriber09=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0010]
Subscriber10=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0011]
Subscriber11=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0012]
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0013]
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0014]
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0015]
Subscriber15=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,SIM24] CHADDR ALARM NODE[0016]
...
```

The CDR can contain the IMSI (International Mobile Subscriber Identity), which identifies each SIM card used:

Example:

```
08.02.05-09:42:15,08.02.05-09:46:19,912345678,01721111111,111111111111111,0101,244,0
```

The following example shows the `pabx.cfg` configuration file changed according to the formula:

Example:

```
...
Subscriber00=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM NEXT
Subscriber01=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber02=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber03=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber04=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber05=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber06=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber07=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber08=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber09=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber10=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber11=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber12=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber13=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
Subscriber14=TRANSPARENT ROUTER GSM[0000,00000,<SMSC>,1,1,1,IMSI,SIM24] CHADDR ALARM
...
```

If you remove the keyword `IMSI` from the `pabx.cfg`, you must restart the system.

To generate a VoIP-call CDR entry that includes IP addresses for the remote device's signaling and voice data, audio codec and frame size, the entry `VoipIpLogging=Yes` must be included in the VoIP profile. If the entry also contains the mobile controller's IMSI, it will appear before the IP addresses.

The following entry shows the `route.cfg` configuration file changed according to the formula:

```
[Voip:DF]
VoipDirection=IO
VoipPeerAddress=192.168.0.2
VoipIpMask=0xffffffff
VoipCompression=g729 t38
VoipMaxChan=30
VoipSilenceSuppression=Yes
VoipSignalling=0
VoipTxM=4
VoipIPLogging=Yes
```

Example: The following CDR entry includes IP addresses for signaling and voice data, audio codec and frame size.

```
21.08.07-11:54:09,21.08.07-11:54:14,40501,[0005:01]toSIM,262032441413482,172.20.25.210:172.20.25.210,G729,20,0101,5,90,0
```

In the case of CDR entries for DLA/Callback calls, the beginning and ending times for the first call leg is always used as the call time. The call time in seconds appears first for the first leg, followed by a slash and the connection time for the second leg.

Example:

```
20.10.05-15:27:36,20.10.05-15:30:36,2621201555555555,DLA1234567890,0101,180/168,10,0
```

11.4.2.2 MISSED CALLS LIST

All incoming calls that are not connected can be recorded in a list to facilitate return calls. Recording is activated using the RRufLog=<name> entry in the pabx.cfg. Specify a file name, e.g. RRufLog=failed.log. Once this setting is made, recording begins at once.

A new line of the following format is created for each incoming call that is not accepted:

DD.MM.YY-hh:mm:ss,src,dst,cause,dur,att

DD – Day	hh – Hour	src – source/extension	cause – reason for tear down
MM – Month	mm – Minute	dst – destination	dur – duration of call attempt
YY – Year	ss – Seconds	service – service indicator	att – number of attempts

```
16.01.05-13:58:52,9030399281679,10111,0101,ff,0,1
16.01.05-14:04:06,9030399281679,10111,0101,91,0,1
16.01.05-14:04:15,9,10111,0101,91,0,1
16.01.05-14:04:39,9030399281679,10111,0101,ff,0,1
16.01.05-14:04:50,903039904983,100,0101,ff,0,1
16.01.05-14:05:02,9030399281679,10111,0101,ff,0,1
16.01.05-14:05:03,9,100,0101,ff,0,1
16.01.05-14:05:14,903039904983,100,0101,91,0,1
20.04.05-16:21:10,[4545]981776,2->10200,0101,ff,0,1
20.04.05-16:21:20,[4545]981776,1->10120,0101,ff,0,1
```

The reason the connection could not be established is specified using DSS1 codes:

91 – (user busy)

ff – call not answered (disconnected by calling party)

When callback with DTMF is configured and no connection is established to the B subscriber, an entry recording the A subscriber's connection time is generated in the failed.log file:

```
20.02.05-10:47:52,[0004:01]00491721234567,[0005:01]DLA0307654321,0101,ff,34,1
```

The CDR contains the IP addresses for signaling and voice data. The first IP address is the signaling address and the second one is the RTP address.The IMSI is written behind the IP addresses if the keyword IMSI is defined in the pabx.cfg:

Example:

```
12.05.05-10:25:51,40,991783,172.20.25.110:172.20.25.110,0101,ff,8,1
```

In the case of missed-call entries for DLA/Callback calls, dur is the connection time for the first leg.

Example:

```
20.10.05-15:00:06,9004930555555,DLA262121111111,0101,92,24,1
```

11.4.2.3 SENDING CDRS VIA E-MAIL

With an appropriate configuration, you can send corresponding CDRs of outgoing and incoming calls as e-mail. Bear in mind that the mail server must be configured in the [Mail] section of the pabx.cfg, as described in Chapter 5.2.2 ⇨. The sender is given as cdr and the system's name appears in the subject box. The text box contains the CDR information according to the format for the entry in Log=/data/cdr.log @<account> @<domain>. A space must appear between cdr.log and @<account>; @<domain> is optional. You can also send CDR entries via e-mail to an e-mail recipient.

Enter an @ sign to send each CDR entry as e-mail:

```
Log=/data/cdr.log @<e-mail account>@<domain>
```

If you enter a ! the entire cdr.log will be sent as an e-mail attachment:

```
Log=/data/cdr.log !<e-mail account>@<domain>
```

11.5 SMS GATEWAY

The SMS Gateway allows you to use your iGATE to send and receive SMS. The following functions are possible with this feature package:

- Sending SMS via e-mail
- Receiving SMS to e-mail, SMS or to a file
- Sending and receiving USSD text messages
- Setting up connections using e-mail
- Sending announcements via e-mail
- Sending automatic SMS for unconnected calls

Bear in mind that the parameters for connection to the SMTP server must be configured in the pabx.cfg's [Mail] section (cf. 5.2.2 on page 72 ⇨).

11.5.1 SENDING SMS VIA E-MAIL

This function makes it possible to send SMS via a iGATE with an ordinary e-mail client. SMS messages are recorded in the CDR log with the service indicator 0500. The destination address with the keyword SMS, the call number, the @ sign and the IP address or the IP name of the iGATE must be entered.

To use this function, you must first set the parameter <smsc> in the pabx.cfg (cf. Table 5.15 on page 65 ⇨).

In the following example, an SMS is sent to the mobile number 015553456789, whereby sms-mail.server.de must correspond with the IP address 172.172.172.172:

Example: SMS015553456789@172.172.172.172 or
SMS015553456789@sms-mail.server.de

The SMS text must be entered in the text box. The subject box is not used. If the e-mail program supports sending the same e-mail to more than one address, the SMS messages are sent in intervals of one second. The iGATE's algorithms evenly distribute the SMS messages to the available mobile modules.

If the iGATE rejects the SMS, an e-mail alerting an aborted SMS will be transmitted to the sender and the attempt will be entered in the corresponding log file (RRufLog=). If transmission is successful, a positive response will be sent when the SMS is accepted by the SMS service center. sent will then appear in the subject dialog. A corresponding CDR will be entered with a destination address beginning with SMS.

A request to set up a connection with the service 'telephony' and the element 'user-to-user' enables the SMS text to be sent to the iGATE. All iGATEs are supported that allow for SMS messages to be sent by the process described above. According to the restrictions of the ISDN signaling protocol, text length is limited to approximately 110-120 characters. Longer texts will be cut off accordingly.

The following entry must appear in the route.cfg configuration file for SMS transmission to be possible: MapAllSMS=<port number>.

Sent SMS will also be recorded if the call log is active on the system. The formats are describe in Chapter 11.4.2.1 ➪ and Chapter 11.4.2.2 ➪.

Example 1 In the following example, SMS-transmission to the number 01721111111 from the e-mail account j.smith was successful:

```
12.07.06-09:59:10,12.07.06-09:59:11,SMS01721111111,j.smith,0500,1,06,0
```

Example 2 In the following example, SMS-transmission to the number 01721111111 from the e-mail account j.smith was unsuccessful. the output -1 as cause value means that no routing entry was configured:

```
12.07.06-09:04:11,SMS01721111111,j.smith,0500,00,-1,0
```

11.5.2 RECEIVING SMS MESSAGES

This function makes it possible to receive SMS messages via a mobile gateway with an ordinary e-mail client, to forward them to another mobile telephone, or to save them to a file.

Bear in mind that you must set the service type in all identical restrict entries.

Example: In the following example, all incoming voice calls are routed to the operator incoming SMS messages are forwarded to the email account `sysadmin`:

```
Restrict26202=100 01
Restrict26202=@sysadmin 05
```

11.5.2.1 SMS TO E-MAIL

The destination number in the iGATE system must correspond with an e-mail account. The e-mail recipient's name contains the keyword 'sms' and the destination number. The subject box contains the SIM card's IMSI and the caller's number.

Example:

From: sms262124915553230618@gsm.teles.de

Subject: SMS 262123203500514 4915553230618

A mapping entry must indicate an e-mail account with a prefixed @. The following syntax is used:

```
Restrict<port>=@<addressee> 05
```

As an alternative, the @ sign can be substituted with a colon (:) in the recipient's address. If only a destination account is given, the configured domain name is used.

11.5.2.2 SMS TO SMS

This configuration makes it possible to forward SMS messages via a mobile gateway to another mobile telephone.

```
Restrict<port>=@-><port><mobile number> 05
```

Example:

```
Restrict20=@->200155512345678 05
```

11.5.2.3 SMS TO FILE

Using this configuration, you can save SMS messages via a mobile gateway to a file.

Make the following entry in the pabx.cfg:

```
MsgLog=/data/msg.log
```

The following entry in the `Route.cfg` is also required:

```
Restrict<port>=@FILE 05
```

11.5.3 INCOMING USSD (UNSTRUCTURED SUPPLEMENTARY SERVICES DATA)

Incoming USSD can either be saved to a file, sent as an SMS to an e-mail address or to a telephone that supports this service.

Make the following entry in the pabx.cfg:

```
MsgLog=/data/msg.log
```

The following entry in the Route.cfg is also required:

```
Restrict<port>=@FILE 06
```

```
Restrict20=@FILE 06
```

11.5.4 SENDING MESSAGES VIA E-MAIL

This function makes it possible to send text messages via the ISDN signaling channel gateway. The destination address with the keyword MSG, the @ sign and the IP address or the IP name of the iGATE system with mobile gateway must be entered.

In the following example, a message is sent to the call number 0123456789, whereby msg-mail.server.de must correspond with the IP address 172.172.172.172:

Example: MSG0123456789@172.172.172.172 or
MSG0123456789@msg-mail.server.de

The message must be entered in the text box. The subject box is not used. If the e-mail program used supports sending the same e-mail to more than one address, the messages are sent in intervals of one second. The iGATE system's algorithms evenly distribute the messages to the available ISDN ports.

If the recipient rejects the call, an e-mail alerting an aborted message will be transmitted to the sender and the attempt will be entered in the corresponding log file (RRufLog=). If transmission is successful, a corresponding CDR will be entered with a destination address beginning with MSG.

A request to set up a connection with the service 'telephony' and the element 'user-to-user' enables the message to be sent to the recipient. All terminal devices and PBXes are supported that allow for messages to be sent by the process described above. According to the restrictions of the ISDN signaling protocol, text length is limited to approximately 110-120 characters. Longer texts will be cut off accordingly.

The following entry must appear in the route.cfg:
MapAllMSG=<port>

11.5.5 SETTING UP CONNECTIONS VIA E-MAIL

This function sets up a connection between subscriber A and subscriber B via e-mail. Subscriber A is identified by an e-mail address and is dialed first. Subscriber B is called when the connection to subscriber A has been set up.

A connection can be set up via e-mail with the keyword 'CALL,' the destination number, the @ sign, and the IP address or the iGATE system's IP name.

The following example shows a connection with the destination number 0123456789, whereby msg-mail.server.de must correspond with the IP address 172.172.172.172.

Example: CALL0123456789@172.172.172.172 or
CALL0123456789@msg-mail.server.de

Any text contained in the text box will be sent to subscriber A as user-to-user information. The subject box is not used.

Subscriber A is identified by an e-mail address and must be activated in the iGATE system. The subscriber's name must appear before the @ sign. This name must be assigned a corresponding MapOut command.

Example: Subscriber's e-mail address is meier@server.de. Subscriber's extension is 555. Configure MapAll@555=meier.

In addition to CTI capability, this function allows for callback via e-mail.

11.5.6 SENDING ANOUNCEMENTS VIA E-MAIL

It is possible to send announcements using e-mail. An audio file with Teles G.711 A-law encoding is simply sent as an attachment. The destination address begins with the keyword `play`, followed by the telephone number, the @ sign and finally the TELES.System's IP address or name.

Example: the e-mail address will look like this:

```
play123456@192.168.0.1
```

or

```
play123456@anouncement.server.de
```

Make the following entry in the route.cfg:

`MapAllplay<number>=<port><number>`

Example: In the following example, a connection to 123456 is set up through controller 9:

```
MapAllplay123456=9123456
```

After the call has been successfully established, the system generates an e-mail that contains the keyword play<num> in the from line. The keyword connected appears in the subject line.

If an error occurs, the keyword error appears in the subject line. For example, errors may occur when the called number is occupied. Bear in mind that the system will attempt to resend the message as often as is defined in the parameter MailToHostRetries.

To distinguish between voice calls and announcement calls in the CDRs, the keyword play appears in front of the DAD in the CDRs.

11.5.7 DISPLAYING INCOMING CALLS

With this function, you can use e-mail to signal incoming calls. Two signaling types are possible:

- Display all incoming calls that receive a busy or ringing signal. Enter the keyword CTI[001.000.000.000] in the VoIP controller's Subscriber line of the iGATE system's pabx.cfg configuration file.
- Display all unsuccessful incoming calls (callback list) that receive a busy signal or remain unanswered. Enter the keyword CTI[002.000.000.000] in the VoIP controller's subscriber line of the iGATE system's pabx.cfg configuration file.

The destination is the address of the called subscriber configured in a corresponding map entry. A callback can be initiated when the recipient responds to the e-mail.

11.5.8 SENDING AUTOMATIC SMS FOR UNCONNECTED CALLS

When the iGATE is implemented in a corporate network and connected to a PBX or between a PBX and the outside line, the following configuration entry in the `pabx.cfg` activates a feature, whereby the system automatically sends an SMS message to dialed mobile numbers that are unreachable or not answering.

A configurable text containing the callers OAD is sent in the SMS message, so that the mobile user knows who called him through the iGATE's interface and can return the call.

The parameter `SMSInfo` activates this feature. The text can be configured on an individual basis, and the caller's number is automatically generated when you enter `%s`. You must enter the text that is to be sent in quotation marks:

```
SMSInfo="<text>%s<text>"
```

No SMS will be generated for unconnected calls if the service code `VOICE` or `DATA` appears in the mapping entry.
The SMS center number must be defined (cf. Table 5.15 on page 65 ⇨), and the routing entry for sending SMS must be configured.
At least two SIM cards must be activated in the iGATE for this feature to work.

Example: In the following example, SMS messages for mobile users are generated only when calls cannot be connected. The network prefix is 0155 and the LAIN is 26212. The company's mobile prefix is 57777.
No other mobile targets for mobile carriers with the LAIN 26212 and 26213 receive SMS, since the parameter VOICE has been defined in the mapping entry:
`pabx.cfg`:

```
SMSInfo="You got a call from %s . Please call back."
```

`route.cfg`:

```
MapAllSMS=26212

MapAll015557777=|26212015557777<<17
MapAll01555=|2621201555<<17 VOICE
MapAll01556=|2621201556<<17 VOICE

MapAll01444=|2621301444<<17 VOICE
MapAll01445=|2621301445<<17 VOICE
```

11.6 PORTED NUMBER SCREENING

Ported Number LCR Extension is a function that enables you to map defined destination call numbers to other destination numbers or networks (number portability). This function is used to allow telecommunications subscribers to change carriers without having to change their telephone numbers.

Number portability is used in the fixed network, as well as in the mobile network. Usually the numbers are mapped in their respective networks. Implementation of this information and the corresponding routing processes result in significant cost savings, as tariff differences between calls to 'normal' and ported subscribers are eliminated.

The database of ported numbers runs on the iMNP, which provides the data online for the entire network. You can also choose an external provieder.

The iGATE automatically routes calls through specific ports, so that all calls through the same carrier (including ported numbers) are routed through the port containing that carrier's SIM card.

11.6.1 SYSTEM REQUIREMENTS

Ported number screening requires the following:

- An active license package for number portability.
- A iMNP server or another appropriate server

11.6.2 ROUTING AND CONFIGURATION

To connect to the number portability database, you must set the entries described in Chapter 5.2.3 ➪.

An appropriate routing entry in the route.cfg file is required to activate Ported Number LCR Extension. This includes activation of digit collection and the following mapping configuration:

```
...
DTMFWaitDial=<sec>
MapAll<num>=|$ph<<<count>
MapAllph=|D@<num><<01
```

The routing entries for the iMNP results contain the keyword QN, followed by the query result, an equal sign and the controller:

```
MapAllQN<query>=<controller>
...
```

Example: The following example uses digit collection (11 digits plus $ph). Every incoming call with a leading digit of 0 results in an iMNP query. The SIM-card LAINs are used instead of controller numbers. All numbers that come back from the iMNP with the LAIN for Carrier_1 (26211) are then routed through Carrier_1's SIM card with CLIR. The same applies for Carrier_2 (26212), Carrier_3 (26213) and Carrier_4 (26214). Numbers that the iMNP sends back as non-existing (00000) are rejected. Numbers that may exist but are not found in the database (99999) are routed as they come in (normal). If the iMNP does not respond within two seconds (D@0), the call is routed as it comes in, whether it is ported or not:

```
DTMFWaitDial=5
MapAll0=|$ph<<14
MapAllph=|D@0<<01

MapAllQN26211=#26211
MapAllQN26212=#26212
MapAllQN26213=#26213
MapAllQN26214=#26214
MapAllQN00000=&81
MapAllQN99999=$normal
MapAllD@0=$normal1
; not in Database
;Carrier_1
MapAllnormal0151=#262110151
MapAllnormal0160=#262110160
MapAllnormal0170=#262110170
MapAllnormal0171=#262110171
MapAllnormal0175=#262110175
;Carrier_2
MapAllnormal0152=#262120152
MapAllnormal0162=#262120162
MapAllnormal0172=#262120172
MapAllnormal0173=#262120173
MapAllnormal0174=#262120174
;Carrier_3
MapAllnormal0155=#262130155
MapAllnormal0163=#262130163
MapAllnormal0177=#262130177
MapAllnormal0178=#262130178
;Carrier_4
MapAllnormal0159=#262140159
MapAllnormal0176=#262140176
MapAllnormal0179=#262140179
```

11.7 SS7-SPECIFIC SETTINGS

This chapter provides a general introduction to SS7, including a description of its basic structure and implementation.

11.7.1 GENERAL SS7 TERMINOLOGY

Table 11.2 ⇨ provides an overview of basic SS7 terms.

Table 11.2 General SS7 Terminology

Term	Explanation
Protocol	A standardized set of rules that govern the logic used for communication between two devices.
E1 line	A line that carries information at a rate of 2.048 MB/second. Each E1 is divided into 32 timeslots, or channels, numbered from 0 to 31.
Timeslot	A unit of 64 Kb/second.

Table 11.2 General SS7 Terminology *(continued)*

Term	Explanation
B-channel	Bearer channel. A channel that carries voice or data traffic.
D-channel	Data channel. A channel that carries signaling.
Link	One or several timeslots carrying signaling.
Trunk	Bundle of bearer channels.

11.7.2 WHAT IS SS7?

SS7 (**S**ignaling **S**ystem #**7**), also known as CCS#7 (**C**ommon **C**hannel **S**ignaling #**7**), is a signaling protocol for calls in a circuit-switched network. SS7 is implemented around the world in most digital networks and is used primarily for communication between network infrastructure devices.

With SS7, signaling links can be individually defined. One SS7 signaling link can handle traffic on many trunks, so that signaling links do not have to follow the same path as the trunks carrying the traffic they handles.

11.7.3 SIGNALING TYPES

There are essentially two types of signaling: associated and quasi-associated.

11.7.3.1 ASSOCIATED SIGNALING

With this type of signaling, the user parts in two signaling points communicate over a direct signaling route, i.e. the signaling route runs parallel to the signaling relation.

11.7.3.2 QUASI-ASSOCIATED SIGNALING

With quasi-associated signaling, user parts communicate over a signaling route consisting of a string of signaling link sets connecting several STPs.

Quasi-associated signaling is the most efficient type of signaling, because it includes all SS7 advantages and eliminates the problems presented by associated signaling.

11.7.4 SIGNALING POINTS

Signaling points (SP) are the nodes in the SS7 network, i.e. switches or other network nodes such as databases.

Each SP is assigned a 14-bit code (SPC), meaning that up to 16384 SPs can be addressed within a signaling network. Three signaling networks, identified by a Network Indicator (NI), can be created for an SP.

A physical node in a network can have more than one SPC. A gateway switch between a national and international signaling network has SPCs from both networks (one international and one national).

There are three types of SP - Signaling End Point (SEP), Signaling Transfer Point (STP) and Service Control Point (SCP).

11.7.4.1 SIGNALING END POINTS

SEPs are the source and destination points of signaling messages, i.e. signaling relations exist between SEPs. All nodes in a telecommunications network exchange signaling information and are, as such, SEPs, regardless of their position in the network hierarchy. Therefore, both local and transit switches can be considered SEPs.

11.7.4.2 SIGNALING TRANSFER POINTS

STPs are network nodes that transfer signaling messages to other nodes without changing the content of the messages. Independent nodes (standalones) can be used to carry out this function in a network, or it can be integrated into an SEP.

11.7.4.3 SERVICE CONTROL POINTS

SCPs form an integral part of IN architecture, providing centralized control of services for an telecommunications network. This enables a network to perform advanced tasks, such as toll-free or pre-paid processing without having to implement the functions on each switch in the system.

11.7.5 SS7 PROTOCOL STACK

SS7 is divided into various parts, which are stacked into levels that resemble the seven OSI (Open Systems Interconnect) layers defined by the ISO (International Standards Organization). Each part of the SS7 protocol stack serves to maintain the network or to deliver the functions it offers.

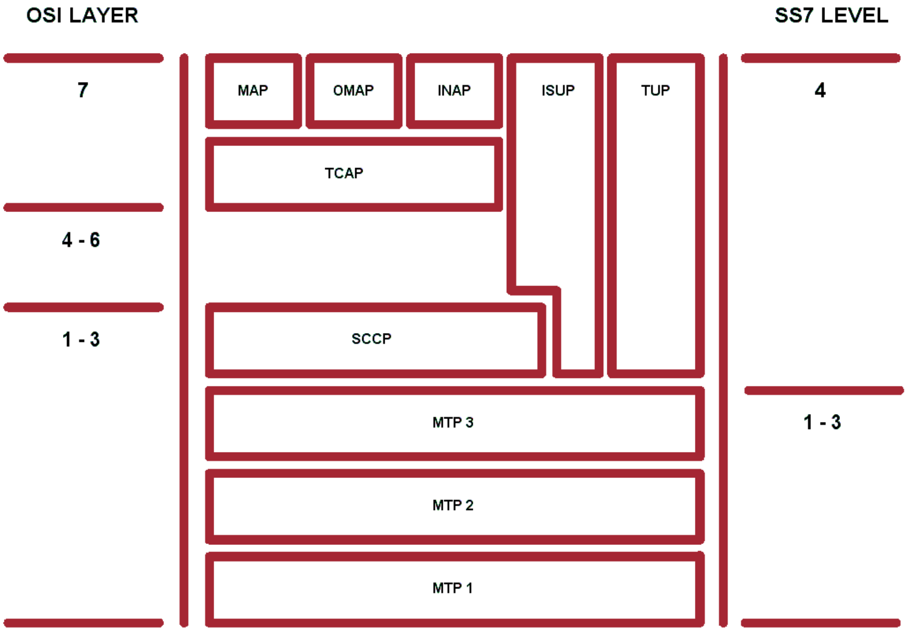


Figure 11.1 SS7 Levels

11.7.5.1 MESSAGE TRANSFER PART

The Message Transfer Part (MTP) provides the basic functions required to transmit signaling messages and manage the signaling network. It consists of the following three levels that must be implemented for the network to function:

MTP Level 1

This is where the physical and electrical characteristics for the network's signaling links are determined and defined. MTP Level 1 can be compared with the OSI Physical Layer.

MTP Level 2

performs the same tasks as the OSI Data Link Layer. It checks the links' functionality and ensures that communication between signaling points is operating properly.

MTP Level 3

contains the functions and procedures for the signaling network, divided into signaling message handling and signaling network management. Signaling message handling switches the messages in the network, while signaling network management is responsible for managing the network and dealing with any problems that occur.

11.7.5.2 ISDN USER PART

ISDN User Part (ISUP) defines the protocol used for connection setup and teardown for all ISDN services and to regulate service indicators. Though its name suggests otherwise, ISUP is used for ISDN and non-ISDN calls.

11.7.5.3 TELEPHONE USER PART

Telephone User Part (TUP) performs most, but not all, of the functions carried out by ISUP. It defines the protocol used for connection setup and teardown for ISDN services and to regulate certain service indicators. TUP is only used for international traffic to specific countries.

11.7.5.4 SIGNALING CONNECTION CONTROL PART

Signaling Connection Control Part (SCCP) handles connectionless and connection-oriented signaling information. The SCCP sets up logical, not physical, connections to exchange local references and SPCs before the physical connection is set up. Together with MTP, it performs OSI layers 1 to 3 tasks. It also provides Global Title Translation (GTT), which translates virtual numbers, like 800 numbers or calling-card numbers, into actual destination point codes and subsystem numbers.

11.7.5.5 TRANSACTION CAPABILITIES APPLICATION PART

Transaction Capabilities Application Part (TCAP), which is transported by SCCP, supports transactions for application processes that are distributed throughout the network. Transaction capabilities are functions and processes that transfer non-user channel network information between different types of facilities. For example, SEPs and SCPs exchange TCAP messages to query and transmit routing information for 800 and other virtual numbers.

11.7.5.6 OPERATIONS, MAINTENANCE AND ADMINISTRATION PART

Operations, Maintenance and Administration Part (OMAP) provides functions for maintenance, service, administration and testing of the individual signaling points. OMAP-defined messages are used to determine the functionality of routing databases and to find inconsistencies in links. They also carry out management functions controlled by a telecommunications management network.

11.7.5.7 MOBILE APPLICATION PART

Mobile Application Part (MAP) is currently the most important user of TCAP. It supports user channel-independent functions, e.g. database queries, in mobile systems, which allow a device to receive and make mobile calls anywhere in Europe without necessarily knowing the current location of the subscriber. This information is stored in a database, which is queried each time a connection is being set up to the mobile number.

11.7.5.8 INTELLIGENT NETWORK APPLICATION PROTOCOL

Intelligent Network Application Protocol (INAP) supports call control within intelligent networks. IN architecture is designed to facilitate the introduction, control and management of new services in an efficient and cost-effective manner. INAP acts as the interface between the various IN functions.

11.7.6 SS7 AND THE IGATE

iGATEs support the SS7 protocol for internal communication between switches in the corporate network. The system is connected to the network as a Service End Point (SEP). The synchronization timeslot is 0. No hardware changes are necessary for SS7 use on a system. Only configuration changes in the pabx.cfg file, as well as a license activation are required.

The following adjustments must be made to the Controller and Subscriber commands in the PABX.CFG:

1. For each of the SS7 ports, add the SS7 keyword to the Controller command after TES2M or NTS2M.
2. Using the Subscriber command, configure the SS7 ports using the following keywords: Subscriber-Port=SS7[OPC,DPC,SSV,SLC,CIC,
   type,ST,STP]
   The point codes (OPC,DPC,STP) can appear in the following format: 4 bit-3 bit-4 bit-3 bit. All other values are hexadecimal, with a leading zero, but no leading format identifier 0x.

Table 11.3 SS7 Keywords

Keyword	Meaning
OPC	Own Point Code: distinctly identifies the port within the corporate network. Use the same four-digit hexadecimal value for each port.
DPC	Destination Point Code: used to distinctly identify the target port within the corporate network. Specify a four-digit hexadecimal number for each port.
SSV	Subservice for the target port: 80 for national – port on the corporate network (NAT0) 00 for international – port on a foreign network C0 for test (NAT1)
SLC	Signaling Link Code: used to distinctly identify the lines running in the same direction on Layer 3. Specify a hex value from 00 to 0F.

Table 11.3 SS7 Keywords *(continued)*

Keyword	Meaning
CIC	Circuit Identification Code: used to identify B channels to the remote switch. Specify a four-digit hexadecimal number.
type	`TRUNK` – standard line (no signaling) `LINK` – for standard usage and signaling in one line For each connection, at least one `LINK` must be configured in correspondence with the configuration used by the remote switch.
ST	Signaling Timeslot: timeslot used for signaling (default 16). Must appear in the following format: `Dxx`, whereby `xx` refers to the timeslot in double digits (e.g. `D16`).
STP	Signaling Transfer Point (optional). You can enter an STP's unique identifier at the end of the square brackets, behind the signaling timeslot. **NOTE: Make sure you do not enter upper-case letters. This entry may never begin with an upper-case D!**

Use timeslots 1-15 and 17-31 as voice channels. Timeslot 16 cannot be used as a voice channel in a trunk configuration.

Table 11.4 Sample of `pabx.cfg`

```
; 5) Controllers
; --------------
Controller00=9 TES2M SS7
Controller01=9 TES2M SS7
; 6) Subscribers
; --------------
; TELES.3PRI board(s)
; ---------------------
Subscriber00=SS7[1-7-a-3,1-7-a-1,80,00,0000,LINK,D16,3-b-2-a] TRANSPARENT ROUTER ALARM
Subscriber01=SS7[1-7-a-3,1-7-a-1,80,01,0020,LINK,D16,3-b-2-a] TRANSPARENT ROUTER ALARM
```

Figure 11.2 ➪ shows four switches communicating via SS7:

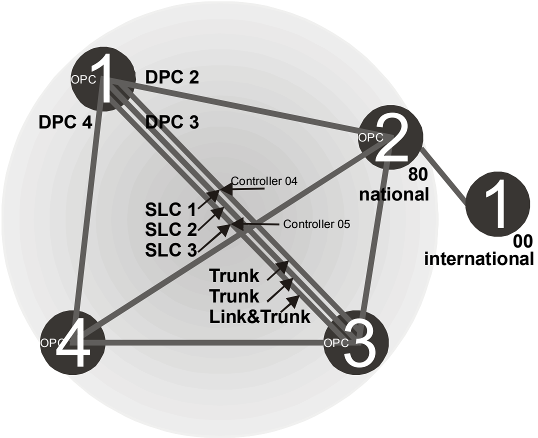


Figure 11.2 SS7 Switch Communication

11.7.7 SS7 ROUTING ENTRIES

It may be necessary for certain options to be sent with SS7 IAMs. These options appear in specific routing entries.

Calls with Continuity Check

A continuity check feature tests a channel to determine if it exists from beginning to end point. Use the following entry for incoming calls with this feature:

```
MapAll<num>=$<pl>
MapAll<pl>W=<port>
MapAll<pl>=<port>
```

A placeholder mapping is set up (`pl`) and a new search of the routing table occurs (`$`). The placeholder `pl` is replaced with a `W` for calls with a continuity check if a `W` appears at the end of the controller's `subscriber` line. Calls without a continuity check are sent directly to the port.

Example: The following example shows a routing configuration in which a continuity check occurs at controller 01.

```
; 5) Controllers
; -------------
Controller00=9 TES2M SS7
Controller01=9 TES2M SS7
; 6) Subscribers
; -------------
; TELES.3PRI board(s)
; --------------------
Subscriber00=SS7[1-7-a-3,1-7-a-1,80,00,0000,LINK,D16,] TRANSPARENT ROUTER ALARM
Subscriber01=SS7[1-7-a-3,1-7-a-1,80,01,0020,LINK,D16,W] TRANSPARENT ROUTER ALARM
```

Example: In the following example, all calls beginning with 0 are mapped to the placeholder pl and sent to port 10 following a new routing-file search. The W routing process is used for calls with continuity check:

```
MapAll0=$pl
MapAllplW=10
MapAllpl=10
```

12 OPTIONAL FUNCTION MODULES

The following modules are included:

- SNMP agent
- DNS forwarder
- ipupdate - DynDNS client

Since these features are only required in individual cases, they are not part of the default software packet. They can be installed as stand-alone modules for the desired function. The description of the functionality of individual modules appears in their respective chapters.

12.1 OVERVIEW

The modules can be downloaded using FTP. The access data for each module is as follows:

- DNS Forwarder
  ftp://195.4.12.80
  user: dnsmasq
  password: dnsmasq
- snmp agent
  ftp://195.4.12.80
  user: snmp
  password: snmp
- ipupdate
  ftp://195.4.12.80
  user: ipupdate
  password: ipupdate

Install the respective software package on the iGATE using GATE Manager. For a description of how to update the software, please refer to Chapter 10.3 ⇨. Make sure the module's file ending is correct before installation. The number in the file ending shows the starting order of the modules. Do NOT change this number if it is 0! All other modules can simply be numbered in ascending order.

For instance, the ending for the optional function module will be tz2 or higher:

- tz2
- tz3

Following completion of transmission, you must adjust the module's configuration and restart the iGATE. Once you have restarted the system, you can use the required features.

12.2 SNMP AGENT

This module allows you to connect the systems and their functions to an SNMP-based network monitoring system. With this module, SNMP requests are answered and alarm messages (E.g. Layer 1 errors on E1 lines) and error recovery messages are sent via SNMP trap.

Traps are generated for all line or mobile ports. The running number in the trap corresponds with the port. The module also monitors whether the voice codec chips are functioning correctly.

The traps for the IP interfaces are also generated in ascending order according to the following list:

Table 12.1 Traps for IP Interfaces

Trap Number	Interface
0	Ethernet 1
1	Ethernet 2
2	Loopback
3	xppp= (if used)
4	pppoe= (if used)

If more than one pppoe<x> profile is configured, the number will also increase.

Bear in mind that the keyword ALARM must be entered in the appropriate PRI, BRI or mobile port's Subscriber line in the pabx.cfg. The MIBs (Management Information Bases) are included on the product CD in the folder MIB. The module name snmpd.tz0 must have the ending tz0!

The following settings are possible in the section [snmpd]:

Table 12.2 Settings in the Section `[snmpd]`

Parameter	Definition
Port=<port>	Defines the target port for the trap server (default 161).
TrapServer=<ip addr>	Enter the SNMP trap server's IP address. Example for listing more than one: `TrapServer=192.168.0.10 192.168.0.12`
Community=<password>	Enter a password for a community (group). The default password is `public`.

12.3 DNS FORWARDER

With this module, the system can function as a DNS server for the clients in the local network. The system in the local network sent the DNS query to the iGATE, which forwards the queries to a known DNS server address if no valid entry for the query is known.

The advantage is that the clients always enter the iGATE's address as DNS server address, so that no public DNS server address is required. The iGATE functions in this scenario as a router.

Of course, the DNS server's address can also be transmitted to the clients using the integrated DHCP server. If the iGATE is used as a DSL router or if it sets up a dial-up connection, no entry is required in the pabx.cfg for the parameter NameServer. The DNS server's address that is negotiated through this connection will be used.

12.4 IPUPDATE - DYNDNS CLIENT

This function allows you to assign a defined hostname to an IP address that changes dynamically. That means that you can always reach a device or service through the public IP network, even if, for example, it is a common DSL connection with dynamic IP address allocation. Several providers support this service.

Make the following entries in the system's ip.cfg, in the [DynDNS] section:

Table 12.3 pabx.cfg: DynDNS

DynDNS Parameters
service=<type> Specifies which provider is used. The following providers are supported: dhs http://www.dhs.org dyndns http://www.dyndns.org dyndns-static dyns http://www.dyns.cx ezip http://www.ez-ip.net easydns http:/www.easydns.com easydns-partner gnudip http://www.gnudip.cheapnet.net heipv6tb hn http://www.hn.org pgpow http:www.justlinux.com ods http://ods.org tzo http://www.tzo.com zoneedit http://zoneedit.com
user=<username:password> Defines the username and password for the DNS service provider.
host=<domain_name_of_dns_service> Enter the domain name that is used.
interface=<If> Defines the interface to be used. Possible entries are `emac0`, `emac1`, `pppoe0`. The dynamic IP address for this interface is transmitted to the service provider.
max-interval=<sec> Defines the value in seconds in which actualization of the name in the DNS database must occur. 2073600 seconds (24 days) is the default value. The shortest interval allowed is 60 seconds. Bear in mind that this setting may cause the provider to block the domain name, since multiple registrations in short intervals are often not allowed. You must clear this with your provider.

Example: In the following example, the DynDNS service is used and the domain name is host.domain.de; the username is user and the password is pwd. The iGATE works as DSL router and the dynamically allocated IP address of the PPPoE interface is used:

```
[DynDNS]
service=dyndns
user=user:pwd
host=host.domain.de
interface=pppoe0
max-interval=2073600
```

Included in the possible uses for this feature is remote access to the iGATE when the IP connection does not have a fixed IP address. In this case, you can access the system, for example with the GATE Manager, if the host name is used in the Remote Number dialog. Example entry in the Remote Number dialog: IP:host.domain.de

TELES AG
Communication Systems Division
Ernst-Reuter-Platz 8
10587 Berlin, Germany
Phone: +49 30 399 28-00
Fax: +49 30 399 28-01
E-mail: sales@teles.com

http://www.teles.com/tcs/