

Edition 1, SW Release 3.2.1 and higher, September 2006

Table of Contents

Manual I: see Installation Guide

Step-by-step guide to install and configure Quadro basically.

Manual II: Administrator's Guide

About this Guide	4
Quadro's Graphical User Interface	5
Administrator's Main Page	5
Recurrent Buttons	6
Recurrent Functional Buttons	6
Entering a SIP Addresses correctly	6
Administrator's Menus	7
System Menu	7
System Configuration Wizard	7
Internet Configuration Wizard	8
Status	10
General Information	10
Network Status	11
Lines Status	12
Hardware Status	14
SIP Registration Status	14
H323 Registration Status	15
IP Routing Configuration	15
Configuration Management	16
Update Configuration	17
Events	18
Time/Date Settings	21
Mail Settings	21
Firmware Update	22
Networking Tools	23
SNMP Settings	24
Diagnostics	25
Automatic Provisioning	26
Upload Language Pack	26
User Rights Management	27
Users Menu	29
Extensions Management	29
Extension Codecs	36
Authorized Phones Database	37
Telephony Menu	38
Call Statistics	38
RTP Statistics	39
SIP Settings.....	40
H323 Settings	40
RTP Settings	41
NAT Traversal Settings	42
Line Settings.....	45
Loopback Settings.....	46
E1/T1 Settings	47
Incoming Interdigit Service	55
Gain Control	55
Call Routing	56
Best Matching Algorithm	61
VoIP Carrier Wizard	64
RADIUS Client Settings	67
Dial Plan Settings	68
System Hold Music Settings	68
Internet Uplink Menu	69
PPP/ PPTP Settings	69
Advanced PPP Settings	69
Firewall and NAT	70
Advanced Firewall Settings.....	71
Filtering Rules	71

Service Pool	73
IP Pool	73
LAN Services Menu.....	76
DNS Settings	76
DHCP Settings for the LAN Interface	76
Registration Form	77
Logout	77
QuadroE1/T1's Feature Codes	78
Establishing a call	78
Using Quadro's PBX Services	78
Administrator Login	78
QuadroE1/T1's Auto Attendant Services	79
Call Codes Available in Auto Attendant	80
Appendix: System Default Settings	81
Appendix: Glossary.....	84
Appendix: Software License Agreement	89

About this Guide

The QuadroE1/T1 Manual is divided into two parts:

- **Manual-I: Installation Guide**

This guide provides step-by-step instructions to provision the Quadro and configure the phone extension with the Epygi SIP Server. After successfully configuring the Quadro, a user will be able to make SIP phone calls to remote Quadro devices, make local calls to the PSTN and access the Internet from devices connected to the LAN.

- **Manual-II: Administrator's Guide**

This guide explains all QuadroE1/T1 management menus. It includes the available call codes and a list of all System Default Values, too.

[Quadro's Graphical User Interface](#) introduces the Quadro's graphical user interface and explains all recurrent buttons.

[Administrator's Graphical User Interface](#) explains each of the Administrator's management on the main page of the Quadro management.

[Quadro's Call Codes](#) describes the Quadro's call codes that enable the user to navigate through Quadro's services from a phone handset.

[Quadro's Auto Attendant Services](#) explains the operation of the Quadro's auto attendant and lists the call codes that may be used to enter the auto attendant.

[Appendix: System Default Settings](#) lists all factory defaults.

[Appendix: Glossary](#) defines some technical terms.

[Appendix: Software License Agreement](#) includes the terms and conditions of using the Quadro's hardware and software.

Quadro's Graphical User Interface

Administrator's Main Page

When the administrator logs in, the **Quadro Management** page is displayed. Here the administrator may access the following settings and perform the following actions:

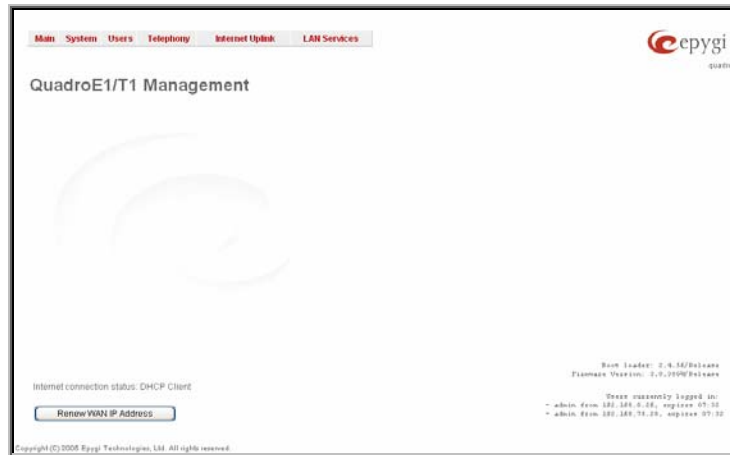


Fig. II-1: QuadroE1/T1 Management

System Menu

- [System Configuration Wizard](#)
- [Internet Configuration Wizard](#)
- [Status](#)
- [IP Routing Configuration](#)
- [Configuration Management](#)
- [Events](#)
- [Time/Date Settings](#)
- [Mail Settings](#)
- [Firmware Update](#)
- [Networking Tools](#)
- [SNMP Settings](#)
- [Diagnostics](#)
- [Automatic Provisioning](#)
- [Upload Language Pack](#)
- [User Rights Management](#)

Telephony Menu

- [Call Statistics](#)
- [SIP Settings](#)
- [H323 Settings](#)
- [RTP Settings](#)
- [NAT Traversal Settings](#)
- [Line Settings](#)
- [E1/T1 Settings](#)
- [Gain Control](#)
- [Call Routing](#)
- [VoIP Carrier Wizard](#)
- [RADIUS Client Settings](#)
- [Dial Plan Settings](#)
- [System Hold Music Settings](#)

Users Menu

- [Extensions Management](#)

Internet Uplink Menu

- [PPP/ PPTP Settings](#)
- [Firewall and NAT](#)
- [Filtering Rules](#)

LAN Services Menu

- [DNS Settings](#)
- [DHCP Settings for the LAN Interface](#)

Registration Form (in menu tree only)

Logout

The button **Renew Wan IP Address** appears on the administrator's main **Quadro Management** page if the Quadro device acts as a DHCP client. The **Renew WAN IP Address** button is used to obtain a new WAN IP address in cases such as the Quadro being moved to another network.

The buttons **Establish Your Internet Connection Now** and **Terminate Your Internet Connection Now** occur on the Quadro Management page if PPPoE is used as WAN interface protocol.



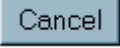
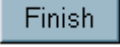


The link **Please Check Your Pending Events** will be displayed on the **Administrator's Main Menu** page when a new system events occurs. The link also leads to the **Events** page that can be also accessed from the **System** menu.





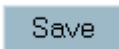

The list of **Users currently logged into the system** is seen in the lower right corner of the **Administrator's Main Menu**. Information about the IP address user accessed Quadro GUI from, the username logged in and the time until the next automatic logout is also seen here. The current version of the Quadro's firmware and of its boot loader is also available here. The idle session timeout is set at twenty (20) minutes. If no action is performed within twenty (20) minutes, the user will be automatically moved to the Login page and will be requested to login again.

The link **Refresh in** is displayed in the upper right corner beside the field displaying the number of seconds remaining until the next refresh and it is used to perform a manual reload of the page. If a page with a Refresh counter is left opened, the session time-out counter will periodically be updated and the logout time will never expire.

Recurrent Buttons

Throughout this guide, you will see a variety of recurrent buttons. Below is a description of these buttons.

Button	Description
	This button leads back to the previous page of a fixed sequence of pages (used mainly in wizards).
	This button leads forward to the next page of a fixed sequence of pages (used mainly in wizards).
	This button discards the latest not yet confirmed entries.
	This is the last button of a fixed sequence of pages that completes and saves the entries of an entire sequence.
	This button opens the help page belonging to the currently active Quadro management page.
	This button opens a window where the last inserted IP addresses are listed. It allows the user to make a quick selection of an IP address that has been previously used. This will avoid the user needing type it again. The clipboard can hold up to 10 IP addresses and a new IP address will replace the oldest one from the list.

Button	Description
	This button returns you to the page you were previously on.
	This button confirms an operation you started before.
	This button confirms an operation you chose before.
	This button discards an operation you chose before.
	This button saves the settings modified on the currently active management page.
	This button opens a window where the last inserted SIP addresses are listed. It allows the user to make a quick selection of an IP address that has been previously used. This will avoid the user needing type it again. The clipboard can hold up to 10 SIP addresses and a new SIP address will replace the oldest one from the list.

Recurrent Functional Buttons

In connection with the tables, the following are the few buttons you will see:

Functional Button	Description
<u>Add</u>	Allows adding a new record to the displayed table. A new page will be displayed to enter any new settings.
<u>Edit</u>	Allows modifying the settings of the record selected by a checkbox. Normally only one (1) record may be selected. A new page will be displayed to enter the modified settings.
<u>Delete</u>	Deletes the selected entry(s) of a table. A warning message will ask for confirmation before deleting an existing entry.
<u>Select All</u>	Selects all table entry(s) for example for further deletion.
<u>Inverse Selection</u>	Inverses (opposites) an existing selection of table entry(s). If no entries are selected, clicking the button will select all records.
<u>Refresh in...</u>	May be shown in the upper right corner of a page. It displays the number of seconds remaining until the next refresh of the page will occur. It may be used to reload the page manually.

Most of the tables offer the option to sort the entries in ascending or descending order by clicking the headings of the columns. A small arrow next to the column heading indicates the direction of sorting - upward or downward. The entries of the table can be selected by using the corresponding checkboxes in order to edit or delete them.

Entering a SIP Addresses correctly

Calls over IP are implemented based on Session Initiating Protocol (SIP) on the Quadro. When making a call to a destination that is somewhere on the Internet, a SIP address must be provided.

SIP addresses needs to be specified in one of the following formats:

```

"display name" <username@ipaddress:port>
"display name" <username@ipaddress>
username@ipaddress:port
username@ipaddress
username
    
```

For your convenience, the following combinations can be used:

- *@ipaddress - any user from the specified SIP server
- username@* - a specified user from any SIP server
- *@* - any user from any SIP server

Attention: Wildcards are available for caller addresses only (for called party addresses no wildcard characters are allowed).

The display name and the port number are optional parameters in the SIP address. If a port is not specified, 5060 will be set up as the default one. The range of valid ports is between 1024 and 65536.

A flexible structure of wildcards is allowed. In comparison with a wildcard, the "?" character stands for only one unknown digit and the "*" character stands for any number of any digits.

Please Note: Wildcards are available for caller addresses only. No wildcard characters are allowed for called party addresses.

Administrator's Menus

System Menu

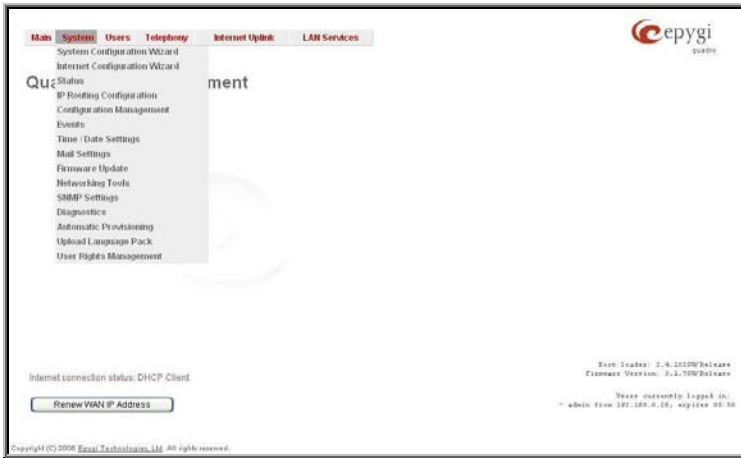


Fig. II-1: System Menu in Dynamo theme



Fig. II-2: System Menu in Plain theme

System Configuration Wizard

The **System Configuration Wizard** allows the administrator to define the Quadro's Local Area Network settings and to specify regional configuration settings to make Quadro operational in its LAN. The **System Configuration Wizard MUST be run upon Quadro's first startup** to make sure that it works properly in its network environment. The Wizard allows navigating through the following basic configuration parameters and settings:

- System Configuration (see below)
- [DHCP Settings for the LAN Interface](#)
- Regional Settings and Preferences (see below)

DHCP Settings for the LAN are described in the chapters below. The LAN configuration and regional settings will be described later in this chapter.

Please Note: It is strongly recommended to leave the factory default settings if their meanings are not fully clear to the administrator.

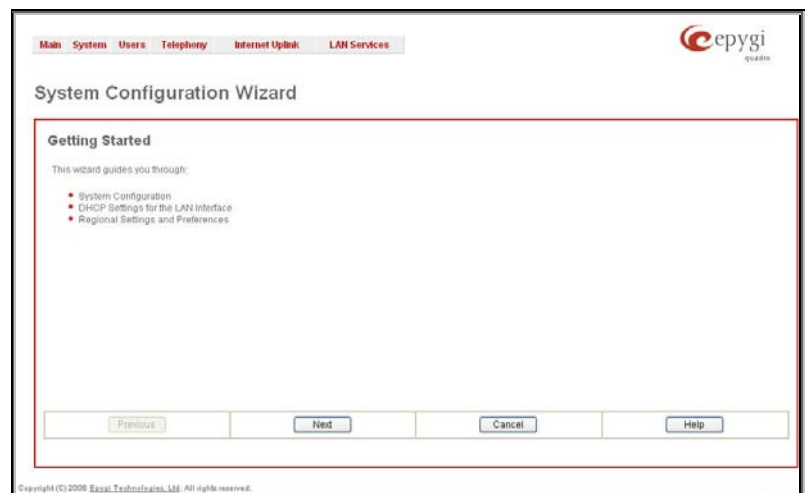


Fig. II-3: System Configuration Wizard - Start page

The **System Configuration** page contains the host name, IP address and Subnet Mask information about the Quadro LAN interface. These settings make Quadro available to the internal network.

The **System Configuration** page offers the following input options:

Host Name requires a host name for the Quadro device.

IP Address requires the Quadro host address for the LAN interface.

Subnet Mask requires the Quadro hosts' Subnet Mask.

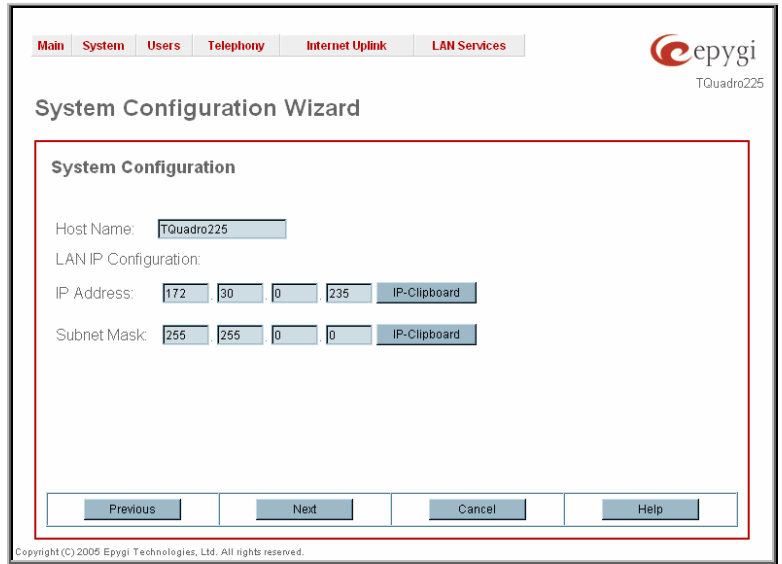


Fig. II-4: System Configuration Wizard - System Configuration page

The **Regional Settings and Preferences** are used to select settings specific to the location of the Quadro. This is important for the functionality of the voice subsystem.

The **Regional Settings and Preferences** page has two drop down lists to select the **Location** (country) and a corresponding **Timezone**. This page also has a radio button group to choose:

- **System Language** – selection is available only when the custom Language Pack has been uploaded and it is used to enable custom language for system voice messages or returning back to the default language English.
- **GUI Theme** - selection used to select the GUI theme style of the web based configuration pages.

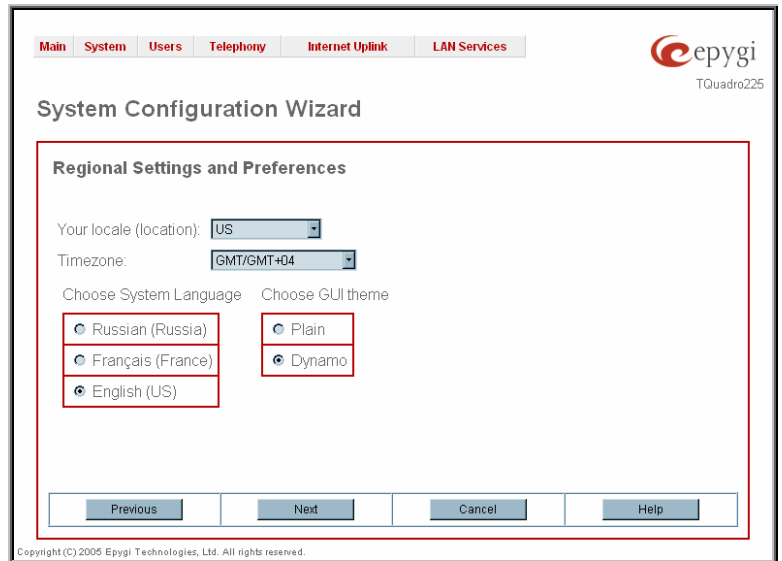


Fig. II-5: System Configuration Wizard - Regional Settings page

Internet Configuration Wizard

The **Internet Configuration Wizard** allows the administrator to configure the WAN interface settings and to adjust Quadro's connectivity with an external network. The **Internet Configuration Wizard MUST be run for Quadro to be connected to the Internet.**

All the settings of the **Internet Configuration Wizard** are described in the chapters below except those for the IP settings, which will be described in this chapter.

Please Note: It is strongly recommended not to change the factory default settings if their meanings are not fully clear to an administrator.

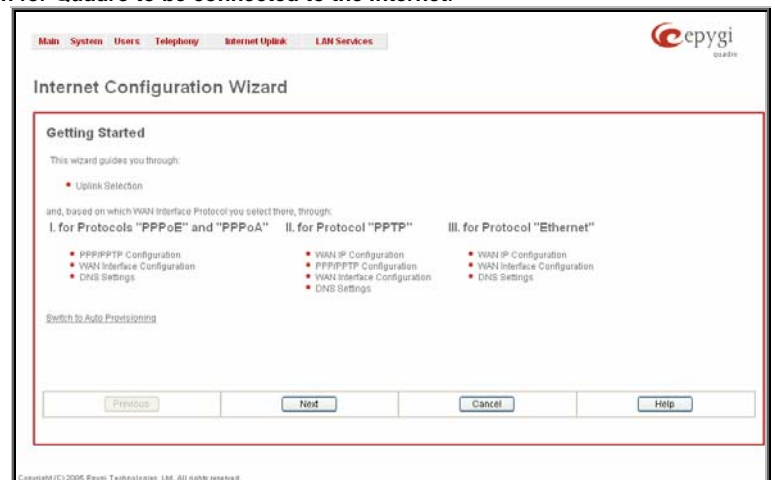


Fig. II-6: Internet Configuration Wizard - Start page

The Wizard allows navigating through the following basic configuration parameters and settings:

- Uplink configuration (see below)

For WAN Interface protocol **PPPoE** and **PPPoA**:

- [PPP/PPTP Settings](#)
- WAN Interface Configuration (see below)
- [DNS Settings](#)

For WAN Interface protocol **PPTP**:

- WAN IP Configuration (see below)
- [PPP/PPTP Settings](#)
- WAN Interface Configuration (see below)
- [DNS Settings](#)

For WAN Interface protocol **Ethernet**:

- WAN IP Configuration
- WAN Interface Configuration (see below)
- [DNS Settings](#)

The **Switch to Auto Provisioning** link moves you to the [Automatic Provisioning](#) page where Quadro can be configured automatically.

The **Uplink Configuration** page allows you to select the Quadro's WAN interface connection type and its bandwidth settings. These settings will make Quadro available to the external network.

Depending on the Uplink Interface Protocol selection, the page following the **Uplink Configuration** page is different. Thus if **PPPoE** is selected, the next page will be **PPP Configuration**, while selecting **Ethernet** will bring up the **WAN IP Configuration** page.

The **Uplink Configuration** page offers the following components:

The **WAN Interface Protocol** radio buttons are used to choose the protocol depending on the requirements of the ISP (Internet Service Provider):

PPPoE - turns on the PPP over an Ethernet connection.

PPTP – turns on the Point to Point Tunneling Protocol (**PPTP**) interface used for the connection between Quadro and ADSL modem. A fixed IP address configuration is needed in this case.

Ethernet - turns on the Ethernet connection.

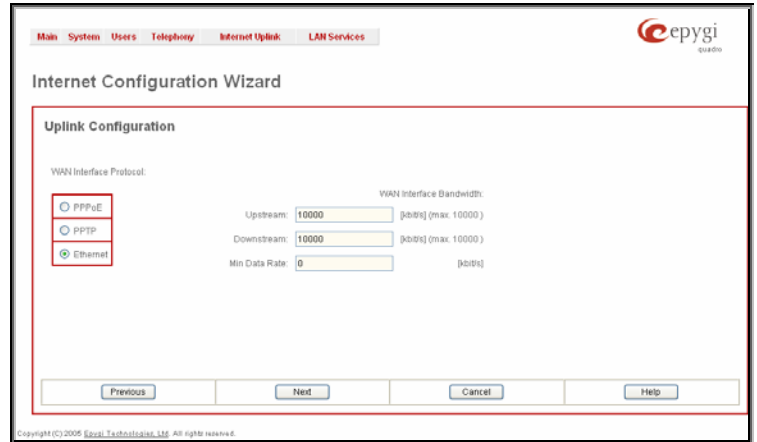


Fig. II-7: Internet Configuration Wizard - Uplink Configuration page

The **WAN Interface Bandwidth** settings allow the specification of the upstream and downstream speeds in kbit/s, helping to assure the quality of IP calls. An IP call loses the voice quality if there is no available bandwidth. When approaching the limits of bandwidth capacity, another IP call will be declined.

The bandwidth provided by the ISP has to be specified in the text fields **Upstream Speed** and **Downstream Speed**. The default entry in both fields is 10000, the maximum bandwidth of a 10 MB Ethernet. In most cases, providers offer a smaller bandwidth than 10000 kbit/s.

The bandwidth required by an IP call depends on the codecs used and these specifications are listed in the table below:

Required Bandwidth for Standard Packets:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:							
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	G.723	iLBC-13.33
10	105	58	66	74	82	50	-	-
20	84	37	45	53	61	29	-	-
30	76	30	38	45	53	22	21	27
40	74	27	34	42	50	19	-	-
50	71	25	32	40	48	17	-	-
60	67	22	30	37	45	15	13	20

The **Min Data Rate** text field requires the amount of upstream bandwidth that ought to remain for data applications even if voice applications use the entire available upstream bandwidth. The value selected here needs to be smaller than the upstream bandwidth and is measured in kbit/s.

The **WAN IP Configuration** page is only displayed if **Ethernet** or **PPTP** has been selected to be the uplink protocol. It offers the following components:

The **Assign automatically via DHCP** radio-button selection switches to automatic retrieval of the WAN IP address from a DHCP server at the ISP/uplink.

Please Note: DHCP referred to here is the one that runs on the provider's side and not the Quadro's personal DHCP server.

The **Assign Manually** radio-button switches to the manual adjustment of IP settings. This selection requests the following parameters:

IP Address requires the IP address for the Quadro WAN interface.

Subnet Mask requires the subnet mask for the Quadro device WAN interface.

Default Gateway requires the IP address of the router where all packets are to be sent to, for example, to the router of the provider.

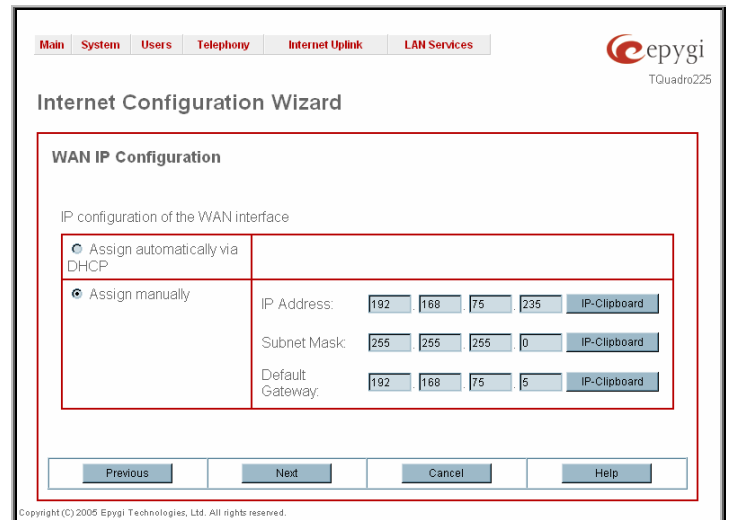


Fig. II-8: Internet Configuration Wizard - WAN IP Configuration page

The **WAN Interface Configuration** page may be used to modify the MAC address of the Quadro. This might be necessary if the ISP (Internet Service Provider) requires a specified MAC address, for example, for authentication. This page offers the following components:

MAC Address Assignment manipulation radio-buttons:

- **This Device** turns to the default MAC address of the Quadro.
- **User Defined** requires user defined MAC Address.

The **MTU** drop down list allows you to select the maximum packet size on the Ethernet (in bytes). MTU is used to fragment the packets before transmitting them to the network. The MTU preferred value is dependent on the Ethernet connection. The default MTU size is 1500 Bytes for Ethernet and 1400 Bytes for PPPoE.

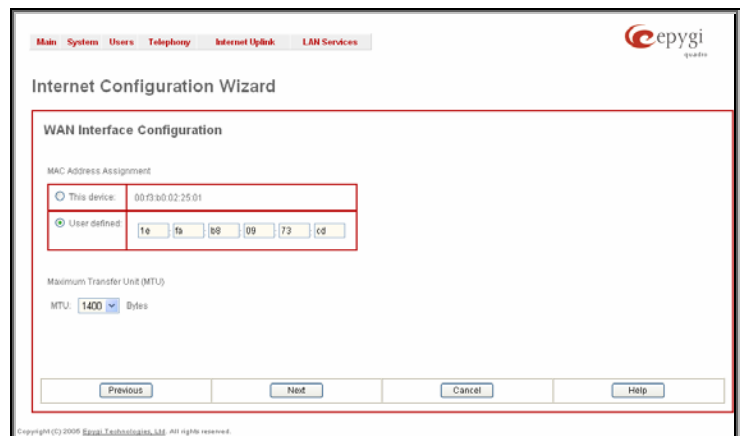


Fig. II-9: Internet Configuration Wizard - WAN MAC Address Configuration page

Status

The system status window displays non-editable tables providing extensive system status information about Quadro: [General Information](#), [Network Status](#), [Lines Status](#), [Memory Status](#), [Hardware Status](#), [SIP Registration Status](#) and [H323 Registration Status](#). The links on this page lead to device Transfer Statistics, user mailboxes and supplementary services configuration pages.

The **System Status** page has several tables providing system information.

General Information

The **General Information** page includes the following information:

- **Uptime duration** - Period Quadro is on since last reboot.
- **Device hostname** - Quadro device host name.
- **Quadro Operating System** - Quadro operating system version.
- **Application Software** - Software and file system versions of the Quadro.
- **Boot Loader** - Quadro boot loader version.
- **DSP Software** - Quadro DSP software version and the date of build.
- **Preinstalled Languages** – this field is present only when multiple languages are preinstalled on the device and it indicates the system default languages.
- **Language Pack** – this field is present only when the custom language pack is uploaded and it indicates the version.

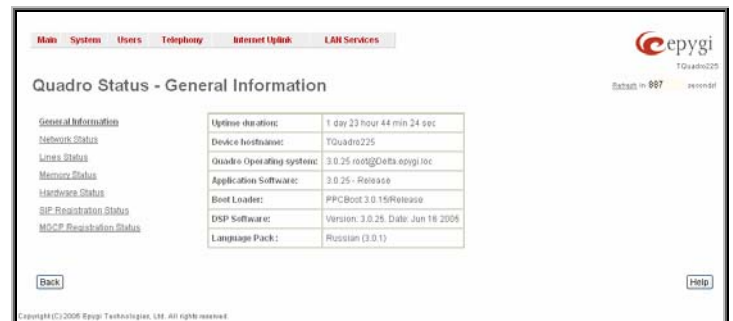


Fig. II-10: Quadro Status - General Information page

Network Status

The **Network Status** page includes the following information about **Interfaces**:

Interface Name lists the Network interfaces available on the Quadro (LAN and WAN).

IP Address lists the IP addresses corresponding to each network interface.

Subnet Mask lists the subnet masks corresponding to each network interface.

Properties will list the MAC address corresponding to each network interface on the Quadro.

Monitor includes links to survey LAN and WAN traffic correspondingly.

- Received Bytes
- Received Packets
- Received Errors
- Received Drop Errors
- Received Overrun Errors
- Received MultiCast Packets
- Transmitted Bytes
- Transmitted Packets
- Transmitted Errors
- Transmitted Drop Errors
- Transmitted Carrier Errors
- Transmitted Collisions

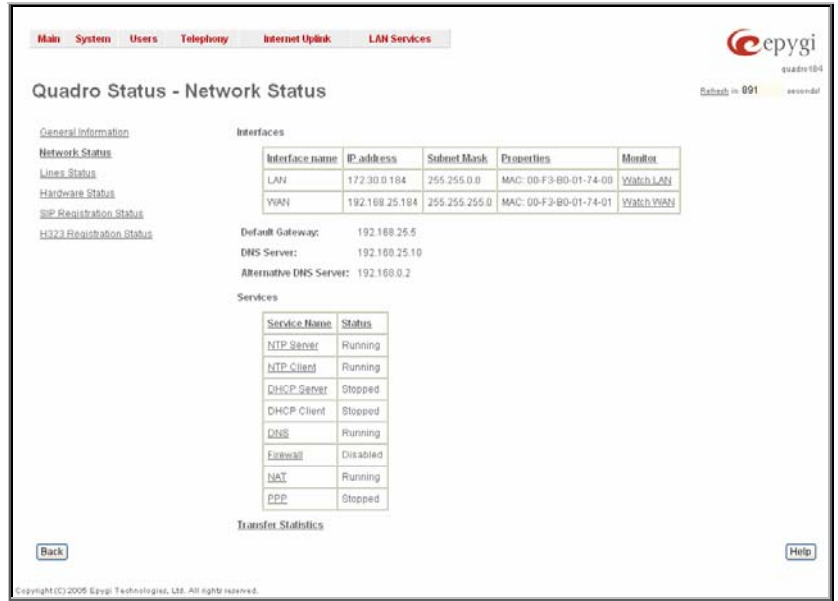


Fig. II-11: Quadro Status Network Status page

When opening the corresponding interface statistics window, no traffic values are displayed at first. After opening the window, the tables will serve as a counter and traffic statistics will be updated every minute.

DNS Server, Alternative DNS Server and Default Gateway - these display the Quadro settings corresponding to what has been configured with the [System Configuration Wizard](#).

Services (NTP Server and Client, DHCP Server and Client, DNS, Firewall, NAT, PPP) statuses: shows if they have **stopped** or if they are still **running**.

Transfer Statistics - link to the Transfer Statistics page.

The **Transfer Statistics** page shows a user-defined statistics table with the transmit/receive value (criteria), interface type and time period. It contains the following components:

Time range of statistic table - the drop down list includes the period (in days) statistics data that is to be collected and the corresponding diagram charts that are to be built.

Interface - the drop-down list offer the values:

- **WAN** - Wide Area Network (WAN) events only
- **LAN** - Local Area Network (LAN) events only

When **Show also as readable values** checkbox is selected, an additional table with statistics values will be displayed on the next page.

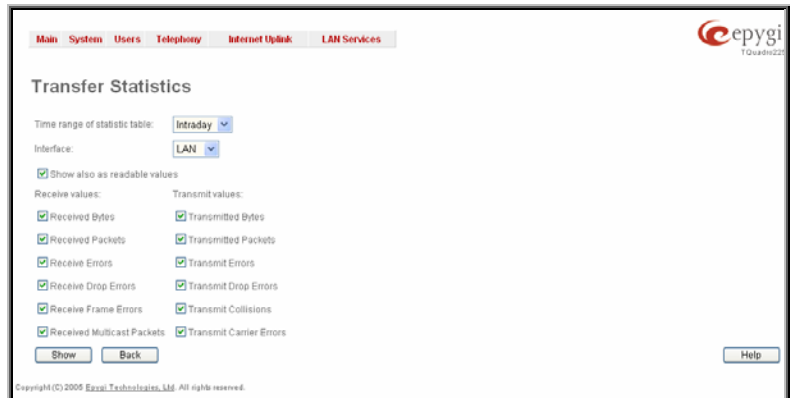


Fig. II-12: Transfer Statistics page

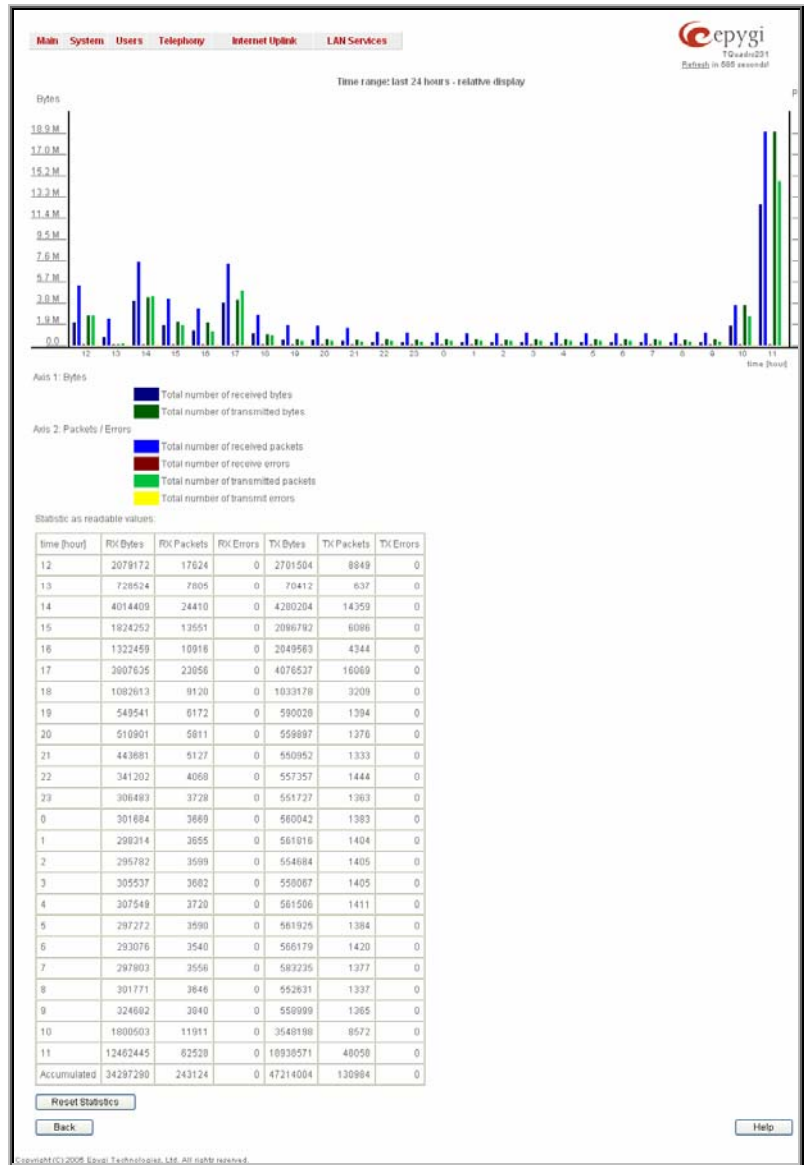


Fig. II-13: Transfer Statistics Diagram Chart

The area **Receive Values** provides the following:

- **Receive Bytes** - number of received bytes.
- **Receive Packets** - number of received Ethernet packets.
- **Receive Errors** - number of received packets containing errors.
- **Receive Drop Errors** - number of received packets that have been discarded.
- **Receive Overrun Errors** - number of received overrun errors that occur when the receive buffer is not large enough to hold all incoming packets. This error usually appears due to a slow receiving system.
- **Receive MultiCast Packets** - number of received broadcast packets.

The area **Transmit Values** provides the following:

- **Transmit Bytes** - number of transmitted bytes
- **Transmit Packets** - number of transmitted Ethernet packets.
- **Transmit Errors** - number of transmitted packets containing errors.
- **Transmit Drop Errors** - number of transmitted packets that have been discarded.
- **Transmit Carrier Errors** - number of transmit carrier errors that occur due to a defective or lost connection on the Ethernet link.
- **Transmit Collisions** - number of transfer errors that occurred during a simultaneous packet transmission from both sides.

To see the **Transfer Statistics Diagram Charts**, select the desired criteria and click **Save** to generate the corresponding chart and the table showing the transfer statistics values (if enabled). The letters **M** (millions) and **K** (thousands) used in the legend of the displayed diagrams show the total number of specified criteria. The **Reset Statistics** button is used to reset the chart and the table (if enabled).

Lines Status

The **Quadro Status - Lines Status** page shows the current status of the extension and E1/T1 trunk. Since only one line information is displayed at a time, the **Phone1** and **E1/T1 Trunk** buttons serve to navigate through information regarding other lines.

The **Lines Status** table displayed for **Phone1** lines includes a group of static and dynamic parameters. Static parameters are displayed always, while dynamic parameters only appear whenever an event takes place on the extension.

Static Parameters:

- Extension** - the extension number of the selected telephone line
- Display Name** – the corresponding name
- Phone State** - On hook or off hook
- Number of Active Calls** – that are currently present on the phone.

Dynamic Parameters:

- Call State** shows the current state of the extension (in voice mail, in call, waiting, busy, call out, ring in, etc.).
- Caller Party** appears when a call is received and indicates the caller extension and the IP address or a phone number, depending on type of call.
- Called Party** appears when a call is placed and indicates the destination extension and the IP address or a phone number, depending on type of call.
- Call Type** shows whether the call is **Internal** or **External** and whether it is a **PSTN** call, **PBX** call or **IP** call.
- Call Start Time** shows the call start date and time.
- Call Duration** shows the current call duration.
- RX Codec** shows the codec used to encrypt the incoming packets.
- TX Codec** shows the codec used to encrypt the outgoing packets. If RX and TX codecs are the same, only one **Codec** field will be displayed.

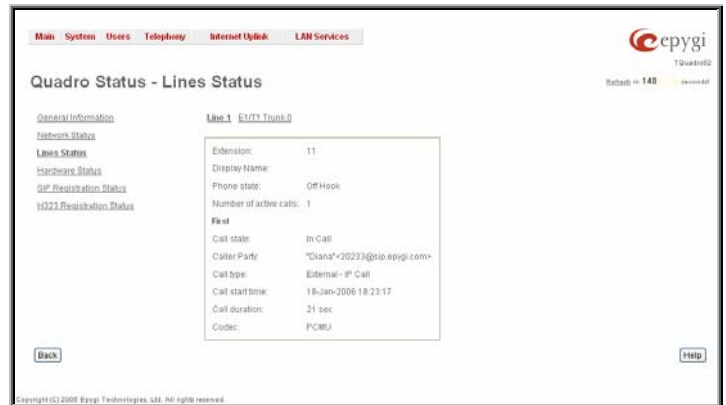


Fig. II-14: Line Status – Line Status page upon established call

The **Line Status** for **E1/T1 Trunk** displays the list of available timeslots (in E1 mode, 30 active timeslots both for CAS and CCS signaling types; in T1 mode, 24 timeslots for CAS signaling and 23 timeslots for CSS signaling type) and their settings (**Route Incoming Call to**, **Allowed Call Type** and **Timeslot State**). When Timeslot is in the call, information about call direction (incoming or outgoing), **Caller Party**, **Called Party** and **Call Duration** is displayed.

All timeslots in the table have an assigned checkbox. The checkbox is used to initiate the DSP capture on one or more timeslots. The “No records selected” error message occurs if you start the DSP capture without any timeslots selected. The **Start DSP Capture** functional button refers to the **DSP Capture** page where the settings of the DSP capture tool on the Quadro can be adjusted as well as captured voice streams can be downloaded. Up to 5 timeslots can be captured at the same time, otherwise if more than 5 timeslots are selected and the **Start DSP Capture** functional button is pressed, the “The number of Timeslots for DSP capture should not exceed 5” error message will appear.

E1/T1 Channel Usage Statistics link refers to the page where traffic statistic table for E1/T1 channel can be composed. It contains the following components:

- Time Range of statistic table** - the drop down list includes the periods (days) for that statistics data is to be collected and for that a diagram chart is to be built.
- Incoming Calls** – indicates incoming E1/T1 call statistics in the output chart.
- Outgoing Calls** - indicates outgoing E1/T1 call statistics in the output chart.
- Maximum Active Calls** – indicates E1/T1 active calls with maximal duration.

To show the **E1/T1 Channel Usage Statistics** select the desired criteria and click **Show** to build the corresponding chart (looks like Transmit Statistics Diagram, see Network Status).

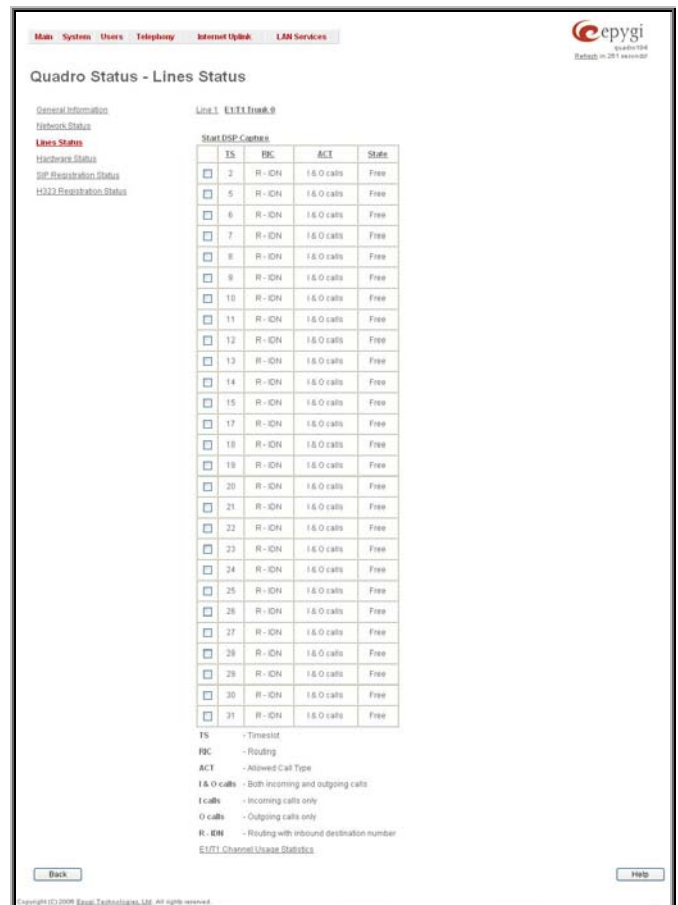


Fig. II-15: Line Status – Line Status page for E1/T1 trunk

DSP Capture

The **DSP Capture** allows you to capture the voice streams transmitted over the selected E1/T1 timeslots. When the page is opened, the DSP capture is already started. To stop the capturing process, use the **Stop** button. The DSP capturing tool's settings can be adjusted only when the capturing is stopped, therefore you need to stop any active capturing to be able to modify the DSP capture settings.

Please Note: Up to 5 timeslots can be captured at the time.

The **Channel Number** text fields are used to indicate the channel number to perform the DSP capture on. Originally the channel number is already filled in depending on the timeslots you have selected. The channel numbering in these text fields starts from 17 for E1 and from 16 for T1, so if you have selected the 2nd and the 3rd timeslots in the E1 mode, 18 and 19 will be filled into the Channel Number 1 and Channel Number 2 text fields correspondingly.

The **Capture Timeout** text field is used to indicate the duration of the DSP capture (in seconds). Once the capture timeout expires, the DSP capturing procedure will stop automatically and the audio files will become available to download from this page.

The **Download Channel # RX** links are used to download the incoming voice streams on the selected timeslots.

The **Download Channel # TX** links are used to download the incoming voice streams on the selected timeslots.

The **Remove Captured Files** link is used to remove all the captured voice stream recordings from the Quadro.

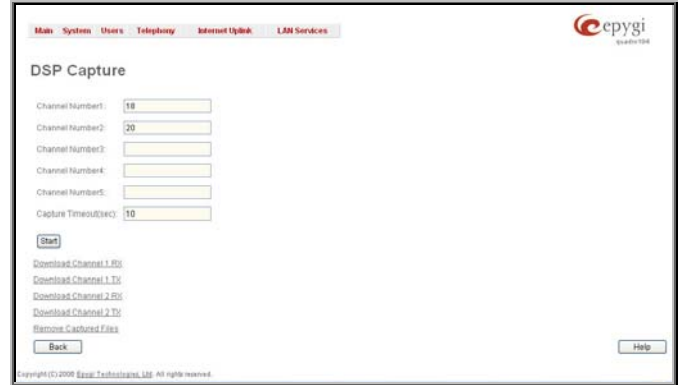


Fig. II-16: DSP Capture page

Hardware Status

The **Hardware Status** table displays a list of the hardware devices present and currently available on the Quadro board. The hardware device version number and additional comments about its state are indicated here.

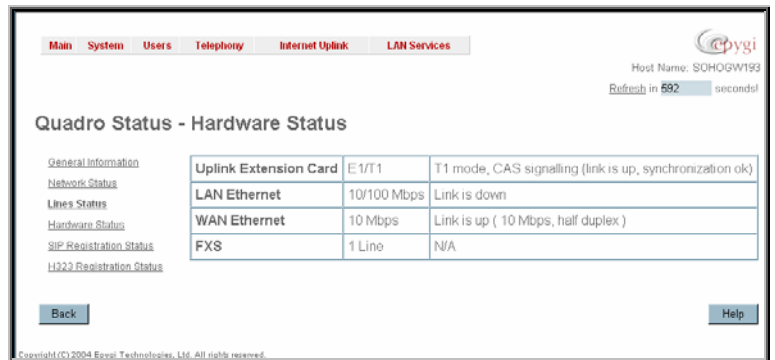


Fig. II-17: Hardware Status page

SIP Registration Status

The **SIP Registration Status** is a table displaying the SIP registration information of the Quadro extensions.

The table contains a list of all the registered extensions of Quadro, SIP registration name for each extension, addresses of SIP servers where they are registered (if applicable), whether or not it is registered for each extension, and the registration date and time. By clicking on the row heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The links inside the table will link you to the [Extensions Management](#) page where the SIP registration settings may be altered.

The **Detected Connection Type** field displays the connection type Quadro currently is acting in (direct connection or behind NAT). If Quadro is acting behind NAT, the NAT machine IP address is also displayed.

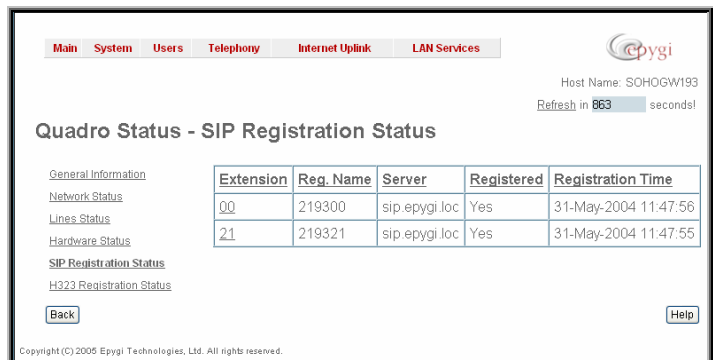


Fig. II-18: SIP Registration Status page

H323 Registration Status

The **SIP registration Status** is a table displaying the H.323 registration status of the Quadro extensions. The table contains a list of all the registered extensions of Quadro, information about H.323 registration states for them, addresses of H.323 gatekeepers where they are registered (if so), registration date and time, as well as H.323 registration names. By clicking on the row heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed next to the column heading.

The links inside the table link you to the [Extensions Management](#) page where the extension's H.323 registration settings may be altered.

The **Detected Connection Type** field displays the connection type Quadro currently is acting in (direct connection or behind NAT). If Quadro is acting behind NAT, the NAT machine IP address is also displayed.



Fig. II-19: H.323 Registration Status page

IP Routing Configuration

Routing is used to relay information across the Internet from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing is different than bridging. The main difference between bridging and routing is that bridging operates at the OSI Data Link Layer (Level Two Media Access Control Layer) and routing operates at OSI Network Layer (Level Three).

Quadro's **IP Routing** service allows you to route IP packets from one destination to another (or to a specified router) through Quadro.

The **IP Routing Configuration** page is used to make IP Static and IP Policy for IP packets routing. This page consists of two tables. Entries in the tables are color coded according to the state of the route. For example, yellow indicates disabled routes, green indicates successful routes and red indicates routes with an error.

IP Static Routes are used to forward IP packets from the Network, where the Quadro is connected, to the specified destination.

The **IP Static Routes** table displays all established IP static routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Route To** for the subnet where the incoming packets should be routed to and **Via IP Address** for the router IP address where incoming packets should be routed through.

Add opens the **Add IP Static Route** page where a new static route can be established.

Enable/Disable is used to activate and deactivate a selected route(s). At least one route should be selected in order to use these functions, otherwise the following error message will appear: "No record(s) selected."



Fig. II-20: IP Static Routing table

The **Add IP Static Route** page offers the following components:

Route To requires the IP address and subnet mask for the destination the IP packet should be forwarded to.

Via IP Address requires the IP address of the subsequent router for IP packet forwarding to the specified destination.

Attention: The rule with the longest subnet (smallest IP range) will take effect when having two or more IP Static routing rules with the coinciding subnets.

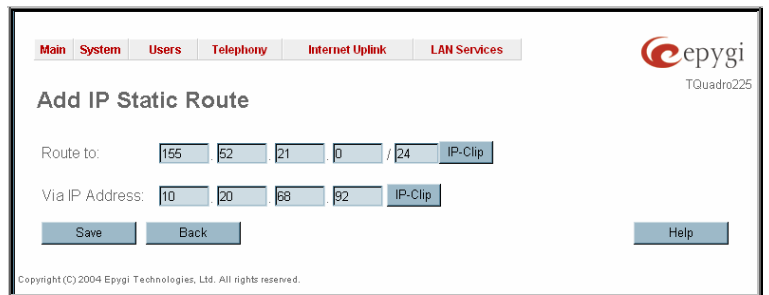


Fig. II-21: Add IP Static Routing page

IP Policy Routes allow IP packets forwarding to the specified router depending on the source IP address as well as defining the priority for the current routing rule.

The **IP Policy Routes** table displays all specified IP policy routes with their parameters: **Target State** for the state of the route (enabled or disabled), **Actual State** for the state of the route connection (up, down or erroneous), **Priority** for the route priority, **Route From** is where the subnet, routed packets come from and **Via IP Address** is where the router IP address incoming packets should be routed through.

Add opens the **Add IP Policy Route** page to establish a new policy route.

Enable and **Disable** are used to activate or to deactivate the selected route(s).

Raise Priority and **Lower Priority** are used to increase or decrease the priority of the selected policy route(s) by one. At least one route should be selected to use these functions, otherwise the error message "No record(s) selected" will appear.

Target State	Actual State	Priority	Route From	Via IP Address
<input type="checkbox"/> enabled	up	15	192.75.10.189/32	192.168.75.225
<input type="checkbox"/> disabled	down	1	155.51.21.0/24	192.168.75.235
<input type="checkbox"/> enabled	up	123	111.323.74.30/24	192.168.75.0

Fig. II-22: IP Policy Routing table

The **Add IP Policy Route** page offers the following input options:

Priority requires a numeric value (from 1 to 252) to define the priority of the routing rule. The lower the number, the sooner the routing rule will take effect (higher priority).

From requires the packet source IP address and subnet mask of the specified destination to match with the rule.

Via IP address requires the IP address of the subsequent router for IP packet forwarding.

Fig. II-23: Add IP Policy Route page

The **Enable** and **Disable** functional buttons are used to activate or to deactivate the selected route(s). At least one route should be selected to use these functions, otherwise the error message appears: "No record(s) selected."

To Add an IP Static Route

1. Select the **IP Static Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Static Routes** page. The **Add Entry** page will appear in the browser window.
3. Enter the destination IP address and subnet mask in the **Route To** text fields. Use the **IP-Clip** button to select a previously entered IP address.
4. Enter the router IP address into the **Via IP Address** text fields.
5. Press the **Save** button to make the static route with these settings.

To Add an IP Policy Route

1. Select the **IP Policy Routes** link on the **Routing Configuration** page.
2. Press the **Add** button on the **IP Policy Routes** page. The **Add Entry** page will appear in the browser window.
3. Specify the policy routing rule priority in the **Priority** text field.
4. Enter the packet source IP address and subnet mask in the **From** text fields. Use the **IP-Clip** button to select a previously entered IP address.
5. Enter the router IP address into the **Via IP Address To** text fields.
6. Press the **Save** button to make the policy route with these settings.

Configuration Management

The **Configuration Management** page assists the administrator with managing the system configuration settings and voice data. For example, the administrator is able to backup and download the settings to a PC and then upload and restore them back to the Quadro. Additionally, this page provides the possibility of restoring the factory default configuration settings.

The **Backup & Download all config & voice data** link generates a backup file with all configuration settings and user uploaded greeting messages. It opens a file chooser window for immediate download to the users PC.

Attention: Configuration and voice data cannot be backed up if the size of voice data is too large. In this case, to be able to backup configuration and voice data on the Quadro, please remove some user defined system messages (by restoring the default ones, see [Administrator Login](#)), or remove some extensions from the [Extensions Management](#) table.

Fig. II-24: Configuration Management page

The **Upload & Restore all config & voice data** link opens a page that has a **Browse** button, (which opens a file chooser to select a backed-up file) and a **Configuration to Upload** field requiring the file path to upload and to restore it immediately. Pressing **Save** will restore the selected backup file, and delete all current user defined greetings and replace configuration settings.

The **Use Default** functional button resets all configuration settings and restores the board's factory default configuration. By restoring the default configuration you will replace your current configuration, lose all voice mails and reboot the device. You will not be automatically redirected to the GUI start page. After the successful reboot you will need to enter into the management page and login again to access the Quadro's configuration. A warning message will ask you to confirm your selection before restoring the default configuration.

Please Note: Unlike the factory default settings restore procedure initialized from the Reset button on the Quadro board, this link will keep the following data:

- Call Statistics
- Transfer Statistics
- System Events
- Feature Keys
- Device Registration state

The [Update Configuration](#) link leads you to the page where Quadro's configuration can be automatically or manually updated, downloaded and edited.

Update Configuration

The **Update Configuration** allows to automatically or manually updating Quadro's configuration, as well as downloading a legible and editable configuration file, making necessary changes and uploading it back to the system. This allows you to use parts of the configuration of one Quadro on another Quadro with some changes done prior to uploading the new configuration. The Quadro reseller, distributor, ISP or carrier usually uses this service.

Attention: It is strongly recommended to consult with the technical support center before making changes on this page. Incorrect settings here may corrupt current configurations.

This page consists of the following components:

Server and **Server Port** text fields require an IP address or Host name and the port number of the server configuration where they will be downloaded from.

The **Update Method** drop down list indicates the connection type used to download the configuration (ftp, tftp, http or https).

The **Enable Version Check** checkbox selection enables version verification before the configuration is being downloaded.

Attention: Disabling the **Enable Version Check** checkbox may cause incompatibility problems on the device.

The **Update Interval Selection** manipulation radio-button group is used to select the frequency of configuration checks/updates performed on the Quadro:

- **Check/Update at boot time** – with this option, new available configuration will be checked/updated each time Quadro boots.
- **Check/Update manually** – with this option, configuration check/upload will be performed only by manual selection.
- **Check/Update time/date scheduled** – with this option new available configurations will be checked/updated periodically depending on the selected time and/or weekday. This selection enables **Time Based** and **Weekday Based** checkboxes. Selecting one or both of them allows you to define the time and the weekday when configuration checks/updates will be automatically performed.

Fig. II-25: Upload Configuration page

The **Update Policy Selection** manipulation radio-button group is used to select the operation performed on the following selections:

- **Check only for update** – with this option, the system will only perform checking of the availability of new suitable configuration and will log corresponding event in the [Events](#) table (depending on configuration in Events Settings).
- **Check and update immediately** - with this option, the system will check the availability and correspondingly update the new configuration and will log corresponding event in the Events table (depending on the configuration in Events Settings).
- **Check and update immediately without any feedback** - with this option, the system will check the availability and correspondingly update the new configuration but will not log any events on this.

The **Check now for new update** functional button performs manual checking of the availability of new configurations and logs corresponding event in the Events table (depending on the configuration in Events Settings).

The **Update now** functional button performs manual checking and update of the availability new configuration and logs corresponding event in the Events table (depending on the configuration in Events Settings).

The **Update now without feedback** functional button performs manual checking and update of the availability new configurations but will not log any events.

The **Download current configuration in a legible format** link refers to the **Configuration Summary** page where a partial or complete configuration can be defined and downloaded or viewed.

The **Configuration Summary** page is used to define a partial configuration and to download it to a PC or to view it directly in the browser.

In the text field on this page, the partial configuration to be downloaded should be specified. Pressing **Start generate a legible configuration file** will start parsing the configuration structure of the device. Progress will be seen in the area below.

The **Cancel generation process** button appears when the configuration generation procedure starts and it is used to stop it.

The **Download generated configuration** button becomes available when the legible configuration generation is finished. It is used to download the generated file to the PC in a plain text format. Necessary changes can be made in the downloaded configuration file and then uploaded back to the system.

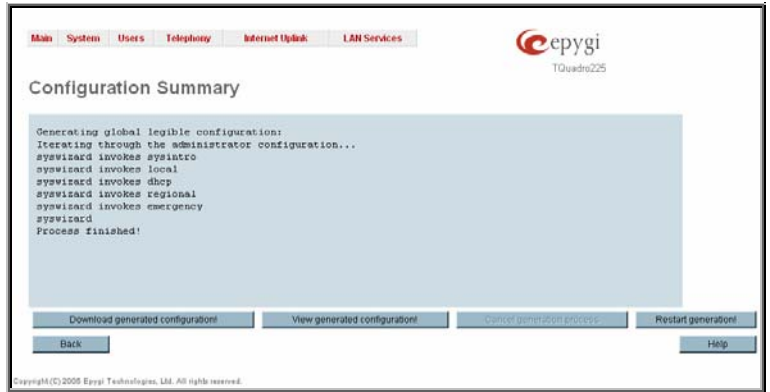


Fig. II-26: Configuration Summary page

Attention: Make sure the changes you have done in the downloaded legible configuration file are valid and will not corrupt the system when being uploaded back to device.

The **View generated configuration** button becomes available when the legible configuration generation is finished. It is used to view the generated file directly in the browser. The **Upload a legible configuration file** link refers to the page where the configuration file can be uploaded in a text format. The **Browse** button in the opened page is used to browse certain legible configuration file to be uploaded and updated to the system. Configuration files to be uploaded should be in the *.txt format, otherwise a system error occurs. The configuration file upload progress will be displayed in the area below.

Events

The **Events** page has two tables. All system events that have occurred will be displayed in one table and event settings will be displayed in the other.

The **System Events** page may be accessed through the **Events** link from the main menu. It lists information about system events that have occurred on Quadro. When a new event takes place, a record is added to the System Event table. For failure events (priority 2 and 3, see below), the warning "Please check your pending events!" will appear at the bottom of all management pages.

The system events and the warning message are visible only for the administrator. The warning link, (which leads directly to the **System Events** page) will disappear from the management pages if the administrator has marked all new events as "read".

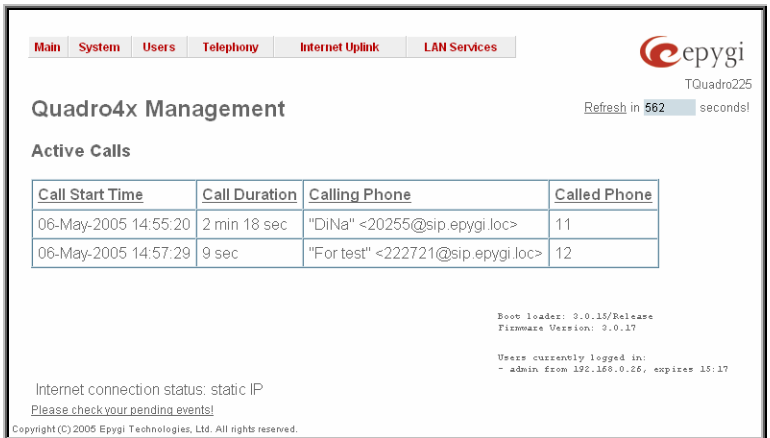


Fig. II-27: Event Warning on the Main Menu page

System Events

Current System Time: Mon Sep 26 15:51:59 2005

Status	Timestamp	Priority	Application	Name	Description	Reference
<input type="checkbox"/>	Mon Sep 26 09:10:29 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epgi.com:5050. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:10:24 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:09:00 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Authentication failure	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Successfully registered user 66101 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Successfully registered user 1100 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Successfully registered user 1102 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:08:55 2005	1	SIP	registration succeeded	Successfully registered user 1101 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:11:01 2005	3	SIP	registration failure	Could not Register user 66101 on server sip.epgi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:11:01 2005	3	SIP	registration failure	Could not Register user 1100 on server sip.epgi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:11:01 2005	3	SIP	registration failure	Could not Register user 1102 on server sip.epgi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:11:01 2005	3	SIP	registration failure	Could not Register user 1101 on server sip.epgi.loc:5060. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:08:34 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:07:34 2005	3	SIP	registration failure	Could not Register user 66101 on server sip.epgi.loc:5060. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:07:34 2005	3	SIP	registration failure	Could not Register user 1100 on server sip.epgi.loc:5060. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:07:34 2005	3	SIP	registration failure	Could not Register user 1102 on server sip.epgi.loc:5060. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:07:34 2005	3	SIP	registration failure	Could not Register user 1101 on server sip.epgi.loc:5060. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:07:04 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epgi.com:5050. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Mon Sep 26 09:05:51 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Destination unreachable	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 02:51:48 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Authentication failure	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 03:19:43 2005	2	SNTP	connect failure	System time could not be set. Reason: None of the servers answered	Time / Date
<input type="checkbox"/>	Sun Sep 25 03:10:49 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 02:41:45 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Authentication failure	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 02:37:26 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 02:36:22 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Authentication failure	SIP Registration Status
<input type="checkbox"/>	Sun Sep 25 02:36:43 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:42 2005	1	SIP	registration succeeded	Successfully registered user 66101 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:59 2005	3	SIP	registration failure	Could not Register user 77 on server sip.epgi.com:5050. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:53 2005	3	SIP	registration failure	Could not Register user 111 on server 111.111.111.111:2123. Reason: Timeout occurred	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:34 2005	3	SYSTEM	reboot	The device has been successfully started after reboot.	
<input type="checkbox"/>	Fri Sep 23 15:29:20 2005	3	SIP	registration failure	Could not Register user 5810 on server sipcenter.com:5060. Reason: Authentication failure	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:25 2005	3	SIP	registration failure	Could not Register user 3330 on server sip.quadrop.net:5060. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:24 2005	3	SIP	registration failure	Could not Register user 51210 on server sip.fwd.com:5050. Reason: Incorrect remote address	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:22 2005	1	SIP	registration succeeded	Successfully registered user 1100 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:22 2005	1	SIP	registration succeeded	Successfully registered user 1102 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:29:21 2005	1	SIP	registration succeeded	Successfully registered user 1101 on server sip.epgi.loc:5060	SIP Registration Status
<input type="checkbox"/>	Fri Sep 23 15:19:35 2005	1	SNTP	time set	Time changed by 1.447249 secs to Fri Sep 23 15:19:33 2005 (09:1.epgi.com)	Time / Date

Fig. II-28: System Events list

The **System Events** table is the list of new and read system events. System events have corresponding coloring depending on the nature of the event: success (priority 1, color green), low importance failure (priority 2, color yellow), critical failure (priority 3, color red).

The table shows the **Status** of the event (new or read) as well as the name of the application the event refers to, event description, and the date when the event was received. For example, if the event was caused due to incorrect mail sending or SIP registration, corresponding links will be seen in the Reference column of the table. The administrator can view the detailed log for each event that has occurred.

The **System Events** page offers the following components:

Current System Time displays the local date and time on Quadro.

Mark all as read marks newly occurred events as "read".

Disable LED switches off the flashing LED (if applicable) on the board. An LED notification may appear (depending on the notification type given) in the page [Events](#) page when a new event occurs.

Numerous circumstances may cause a certain application on Quadro to flag an event.

The **Event Settings** page lists all possible events on the Quadro and allows controlling notification (action) when an event takes place.

Each entry in the events' table has a checkbox assigned to each row. By selecting the corresponding checkboxes, operations such as **Edit** may be done for one or more events.

Edit opens the **Edit Event Settings** page to modify the event action.

Display Notification - A notification link will be displayed on the bottom of all pages and a record is added into the **Events** table. The notification is executed as a link "Please Check you pending events!". The link leads to the **System Events** page. This action also will take place if Flash LED or Send Mail has been selected, even if not specifically selected.

Flash LED - The second LED (yellow) will blink every second and a notification will be displayed on the bottom of all pages. For some events the LED will start flashing after a delay.

Send Mail - A notification e-mail about the new event description in the email will be sent to the e-mail address specified in the **Mail Settings** page.

Send SNMP Trap - an SNMP notification will be sent to the traphost(s) listed in the **SNMP Trap Settings** table (see **SNMP Settings**).



Fig. II-29: Event Configuration Settings page

Actions that are not allowed for the selected event (like mail notification if the PPP link is down or the mail server has been configured improperly) are hidden. For multiple events editing, actions that are not appropriate for least one of the selected events will also be hidden.

If Quadro cannot receive an IP address from the DHCP or PPP servers, or cannot register an extension on the SIP or Routing servers, or cannot reach an NTP server, it raises only one event for the entire period the action has failed, but will continue to try. When the required action is successful Quadro raises an appropriate message.

The **Edit Event Settings** page offers the following input options:

Application displays the application the event refers to. **Multiple** is shown here if more than one event has been selected for the action assignment.

Name displays the name of the event. **Multiple** is shown here if more than one event has been selected for the action assignment.

Description displays additional information about the event. **Multiple** is shown here if more than one event has been selected for the action assignment.

Action offers radio buttons to choose one of the actions to notify the Quadro administrator when an event(s) takes place.

To Assign an Action to the Event

1. Select the checkbox of one or more events to assign an action to them.
2. Press the **Edit** button. The **Edit Event Settings** page appears.
3. Select an action type from the **Action** radio buttons to notify the administrator about the event.
4. Press the **Save** button to submit the changes or use **Back** to abort the selected action.



Fig. II-30: Edit Event Settings page

Time/Date Settings

The **Time and Date Settings** page provides information about the current system time and date. The settings may be updated through the international time and date servers.

Time is used to set the local time (hour, minute).

Date is used to set the date (month, day, year).

Timezone provides a selection of world time zones and is used to select the local country time zone. Timezones are specified by GMT (Greenwich Mean Time) and by specific timezones for the United States and Canada.

Enable Simple Network Time Protocol Server enables the SNTP (Simple Network Time Protocol) server on Quadro, thus Quadro becomes the timeserver for its LAN.

Enable Simple Network Time Protocol Client enables the SNTP client on the Quadro, thus Quadro becomes a client to an external timeserver. A checkbox disables Date and Time drop down lists and enables the following parameters:

The **SNTP Servers** table lists all defined NTP Servers.

The **Add** functional button opens an **Add NTP Server** page where a new NTP server can be defined. This page offers the **NTP Server** radio buttons that are used to choose between a manual and a predefined NTP server.

Manual requires the NTP server's FQDN (Full Qualified Domain Name) or its IP address.

Predefined is used to select the NTP server's host address from the drop down list, where the most common NTP servers are listed.

The **Move Up** and **Move Down** functional buttons are used to sort NTP servers in the order they need to be accessed. If the NTP server in the first position of the **SNTP Servers** table does not answer, NTP server in the next position will try to be reached.

Please Note: You can add another NTP server to the list if the defined NTP servers are not functional (for example, Quadro's date/time is not being updated automatically).

Polling Interval indicates the time interval for the periodical synchronization between the timeserver and Quadro. It counts in hours.

Attention: **Time and Date Settings** will be reset if Quadro has lost power.

Mail Settings

The **System Mail Settings** page allows you to send warnings automatically about the board status or problems to the administrator. System events that require email notification are selected on the [Events](#) page. System mail must be enabled and the SMTP server needs to be configured for voice message transmission to the extension user's mailing account.

Enable enables system mail sending and voice messages transmission to the extension user's mailbox.

SMTP Host requires the SMTP host IP address or domain name. The SMTP host needs to be configured to enable voice message transmission.

SMTP Port requires the SMTP host port number.

Mail Sender Address text field requires the source address for the Quadro notification emails. The email address defined here should be an existing valid e-mail address registered on the selected SMTP server or it should have permission to use that particular SMTP server for e-mail transmission.

Mail Recipient Address text field requires an active e-mail address where system emails will be delivered. The e-mail recipient here can be a Quadro administrator or someone responsible for network and system problems.

Fig. II-31: Time and Date Settings page

Fig. II-32: Add NTP Server page

Fig. II-33: System Mail Settings page

Mail Recipient Address (CC) text field requires an active email address where a carbon copy (CC) of the system emails will be delivered.

Enable SMTP Authentication must be selected if the specified SMTP server requires authentication. In this case, authentication **User Name** and **Password** configured on the SMTP server should be defined in the corresponding text fields.

Send Test Mail is used to initiate a test e-mail transmission. This button will be enabled if correct values have been submitted and saved on this page.

To configure the System Mail

1. Enable the system mail sending by the **Enable** checkbox selection.
2. Update or set the SMTP host in the **SMTP Host** text field.
3. Update or set the e-mail sender address in the **Mail Sender Address** text field.
4. Update or set the e-mail address in the **Mail Recipient Address** text field.
5. Enable **SMTP Authentication** if it is required on the server.
6. Insert into the corresponding text fields an authentication **User Name** and **User Password** defined by your SMTP server.
7. Press the **Save** button to submit these settings.
8. Use the **Send Test Mail** button to send a test e-mail with the configured settings.

Firmware Update

This window allows updating the software of Quadro by installing new firmware (image). Users registered at Epygi will receive a notice when new firmware is available and will be able to download it from the Epygi Technical Support WEB page.

Updating new firmware requires a working power supply. Quadro is provided with a battery (accumulator). If the battery is low or simply absent the "There is no battery or voltage is low" warning is displayed.

Please Note: Installing new firmware will take about 15 minutes. During this time, QuadroE1/T1, telephony and Internet access will be disabled.

The firmware update will cause the loss of the following data:

- All internally stored voice mails and custom voice messages
- DHCP leases
- Transfer statistics
- Call statistics
- All pending events
- User specific GUI states

The following main processes will be stopped during the firmware update and will be restarted after the installation is completed:

- Voice Software
- Network Time Protocol Daemon
- Network Interface Statistic Daemon
- Dynamic DNS Daemon

Please Note: If you consider the [Call Statistics](#) entries in the displayed tables to be important, it is recommended to download them from the corresponding page prior to starting the Firmware Update.

Next will move you to the second page of Firmware Update where the image file should be selected.

The second page of **Firmware update** has the **Browse** button used to browse the image file, and the **Specify Image** text field that will display the selected image filename.

Pressing **Save** will start uploading the image file to the board and the next page will display results and verification of the image being burned.

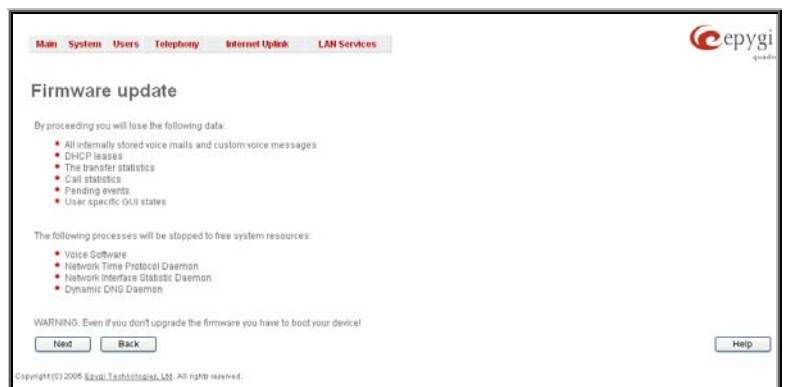


Fig. II-34: Firmware Update page 1

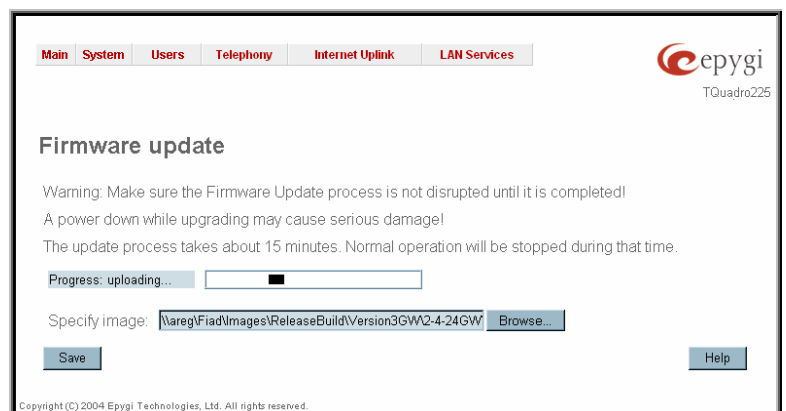


Fig. II-35: Firmware Update page 2

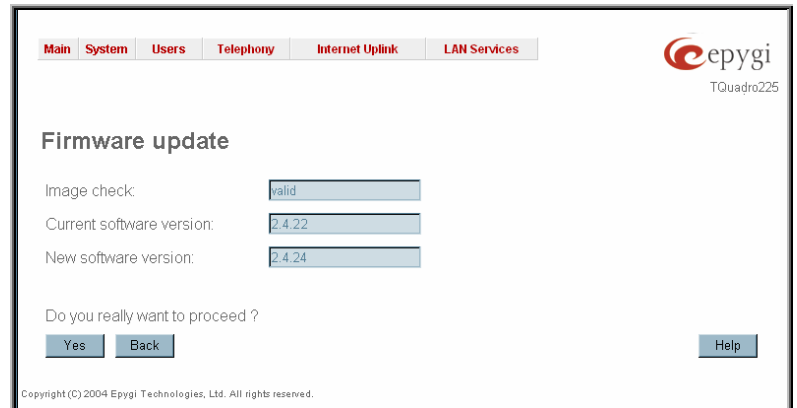


Fig. II-36: Firmware Check page

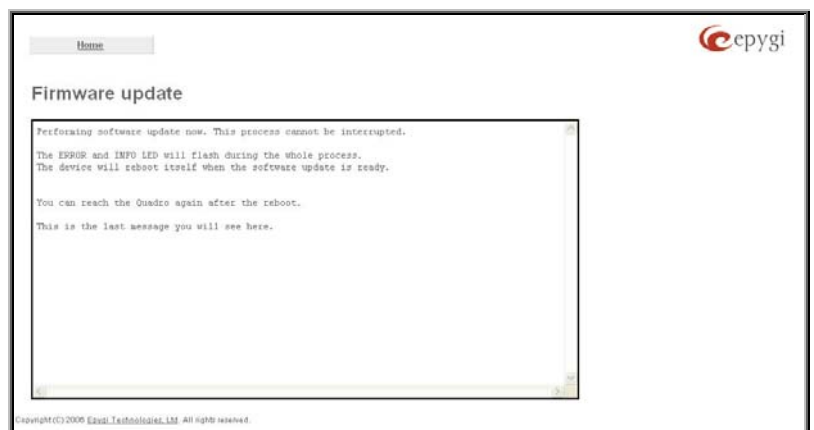


Fig. II-37: Firmware Update page

This page displays non-editable information about the image validity. The **Image Check** field will display "invalid" if the image does not correspond to the hardware version.

The **Current Software Version** field shows the old software version. The **New Software Version** field shows the new version of the software image.

This page needs to be confirmed in order to continue image updating. If you are sure that the image version is appropriate for your device press **Save**.

If you have confirmed the firmware version, a new page with firmware update progress will be displayed next. There are no functions available on this page, just information about the firmware update procedure. At some point the connection with the device is being lost and you need to wait until the firmware will be burned on the Quadro.

You will not be automatically redirected to the Login page. To access the Quadro's Web GUI, you need to connect Quadro again and login.

Networking Tools

The **Networking Tools** page provides the possibility to check the Internet connection.

Ping sends four ICMP (Internet Control Message Protocol) requests with a default size of 64 bytes to the destination (IP address or host name) specified in the text field **Ping Target**. The response times are logged, and the round trip time (the time required from being sent until being received again) is measured. The minimum and maximum round trip time and its average as well as the percentage of lost and of received frames results are displayed in the lower area of the page.

Traceroute checks the Internet connection by triggering the routers (hops) that are passed to reach the destination specified in the **Traceroute Target** text field. Trace routing gives feedback on the routers passed by packets on the way toward the destination and the round trip delay of packets to these routers.

Attention: No **Traceroute** is possible if a high priority Firewall has been enabled (see chapter [Firewall and NAT](#)).

For the purpose of tracerouting, several IP packets are sent out. UDP (User Datagram Protocol) is used to send packets and ICMP (Internet Control Message Protocol) is used to receive information about the routers. In their headers, the TTL (Time To Live) value increases from 1 to 30. When the first IP frame is received by the first router, its IP address will be returned in its acknowledgement.

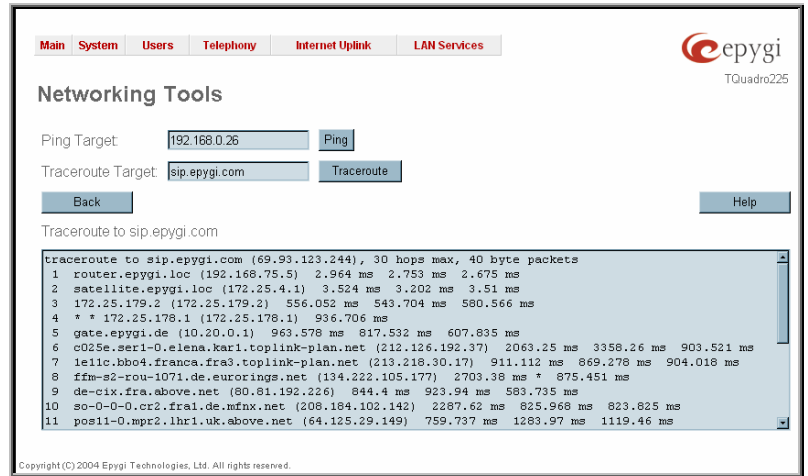
The second frame delivers the IP address of the second router and so on and so forth. The results of **Traceroute** are displayed on the lower area of the page.

Ping Target requires the destination (IP address or host name) for the ICMP request. The **Ping** button starts pinging the specified ping target.

Traceroute Target is used to enter the IP address or host name of the destination to be trace routed.

The **Traceroute** button is used to process the router triggering to check the Internet connection.

In the field below these, the output of the Ping or Traceroute procedure is shown.



To Check the Internet connection

1. Specify the destination address for the ICMP request in the **Ping Target** text field.
2. Press the **Ping** button to process the ICMP request.
3. Specify the destination address to trace the route.
4. Press the **Traceroute** button to process the router triggering.

SNMP Settings

The **Simple Network Management Protocol (SNMP)** is an application layer protocol that facilitates the exchange of management information between network devices and is used by network administrators to manage network performance, find and solve network problems, and plan for network growth.

On Quadro, SNMP agent is running to allow administrators to remotely manage Quadro's network and the device's configuration. Remote administration is being performed by means of special SNMP monitoring programs (SNMP Manager), which can automatically feedback by the certainly configured actions on some events on the Quadro or remotely modify Quadro's settings.

SNMP Settings page is divided into two pages: **Global SNMP Settings** and **SNMP Trap Settings**.

Global SNMP Settings are used to enable the SNMP agent on the Quadro, to select the SNMP protocol version for communication with the administrating application and to define the community for administrating application to connect the Quadro.

Enable SNMP checkbox is used to enable SNMP agent on the Quadro.

System Location text field requires optional information to describe the network where SNMP management is performed.

System Contact text field requires optional information about the contact person responsible for the SNMP management in the defined network. Field may indicate the point person's name, email address, phone number or other contact information.

Enable SNMP v1 / 2c checkbox is used to enable SNMP v1/2c protocol version for the messaging between Quadro's SNMP agent and the administrating application. If this checkbox is not selected, **SNMP v1** will be implied.

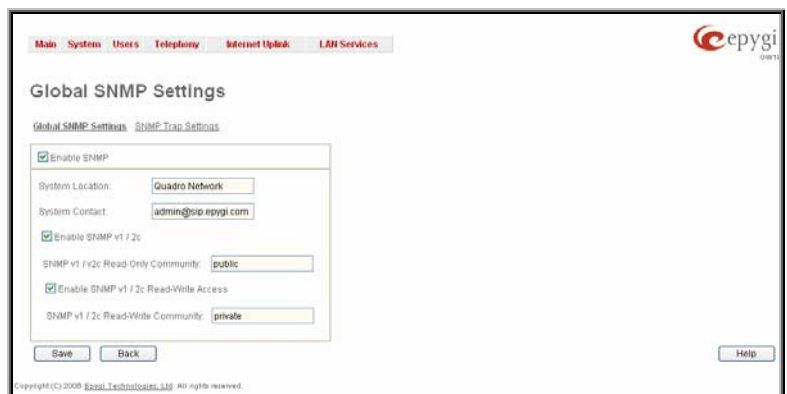


Fig. II-39: Global SNMP Settings page

SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about Quadro's). Field may contain some kind of password which should be matching both on Quadro and on the administrating application for successful SNMP management.

Enable SNMP v1 / 2c Read-Write Access checkbox additionally enables a read-write access on the Quadro for the SNMP monitoring application. With this checkbox enabled, administrator will be able to remotely configure the Quadro via SNMP administrating program.

SNMP v1 / v2c Read-Write Community text field is used to insert the community description (public, private, etc.) for the read-write management (like gathering information (events, statistics, etc.) about Quadro's and remotely changing Quadro's configuration). Field may contain some kind of password which should be matching both on Quadro and on the administrating application for successful SNMP management.

SNMP Trap Settings are used to define the traphosts that should be informed when certain events occur on the Quadro. For the listed traphosts to be informed about the events on the Quadro, **Send SNMP Trap** action should be configured for the corresponding event(s) from the [Events](#) page.

SNMP Trap Settings page contains a list of all configured traphosts with the referring information.

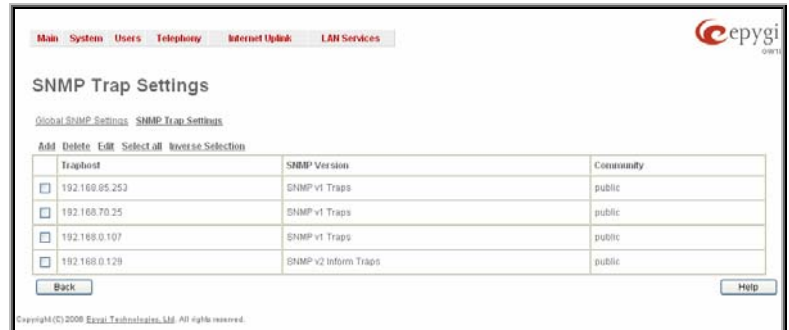


Fig. II-40: SNMP Trap Settings page

Add functional button is used to add a new traphost to the table and opens **Add SNMP Traphost** page where the new traphost might be defined. Page consists of the following components:

Traphost text field requires an IP address or the host name of the traphost. Administrating application's host address should be inserted here.

Community text field requires community description (public, private, etc.) for the administrating application to accept the notifications about the certain events on the Quadro. Field may contain some kind of password which should be the same both on Quadro and on the administrating application for successful SNMP management.

A group of radio buttons is used to select the SNMP protocol version used for events notifications delivered by the Quadro to the administrating application.



Fig. II-41: Add SNMP Traphost page

Diagnostics

The **System Diagnostic** page gives a possibility of running Network and WAN protocol diagnostics to verify Quadro's connectivity and to download all system logs for possible problems recovery.

The **Start Detecting WAN Protocol** button is used to initiate WAN diagnostics that will detect the WAN IP configurations: static or through DHCP and PPP servers. For static WAN IP configuration, gateway availability is checked. When acting as a client, DHCP and PPP servers' accessibilities are being verified.

The **Start Network Diagnostics** button is used to initiate network diagnostics, i.e., to check the WAN link and IP configuration, to verify gateway, DNS primary and secondary (if configured) servers' accessibilities.

The **Start E1/T1 Diagnostics** button is used to initiate E1/T1 **Link Diagnostic** and **Diagnostic Loopback**. With these tests E1/T1 physical link is checked, Frame Synchronization and Red Alarm states are verified. For successful **Link Diagnostic**, remote side should have `Line_loopback` or `Payload_loopback` settings configured or a loopback terminator should be plugged to the Quadro's E1/T1 port. **Diagnostic Loopback** will be initiated if **Link Diagnostic** is failed or E1/T1 link is down.

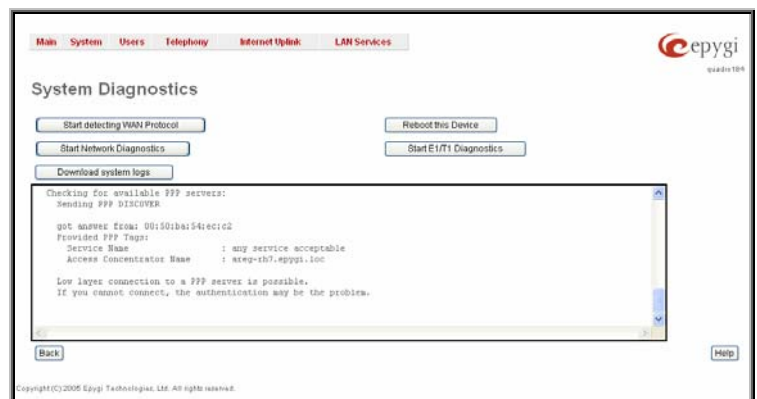


Fig. II-42: System Diagnostic page

The field below will display the diagnostics results and the connectivity conditions. The system should be reconfigured if problems occur during the diagnostics.

The **Download system logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your Quadro.

The **Reboot this Device** button is used to reboot the Quadro. Please note that the session with the Quadro will be closed, i.e., the Quadro GUI should be newly opened and a new login will be required afterwards.

Automatic Provisioning

Automatic Provisioning provides the possibility to automatically configure the WAN network settings of Quadro. This is very useful when the administrator is not actually aware about the Quadro's network settings. **Automatic Provisioning** automatically detects the matching network configuration settings, applies them on the Quadro, thus connecting the device to the internet through the available ISP connection.

Please Note: **Automatic Provisioning** can only be run from the LAN side of the Quadro, i.e. from the PC connected to the Quadro's LAN.

Automatic Provisioning automatically detects and configures the following settings on the Quadro:

- WAN interface type (PPPoE or Ethernet)
- WAN IP settings
- PPP settings
- ISP settings
- DHCP settings
- DNS settings
- NAT Traversal settings

Upload Language Pack

The **Upload Language Pack** page allows you to upload a custom language for GUI and Voice Messages of the Quadro. The language of voice messages can be switched to the custom Language Pack language from the GUI setting page in the [System Configuration Wizard](#). The language of GUI session can be changed to the custom Language Pack language from the radio buttons on the login page.

Uploading a Language Pack will cause the loss of the following data:

- All internally stored voice mail
- DHCP leases
- Call statistics
- Pending events
- Transfer statistics

Please Note: Only one custom Language Pack can be uploaded at the time. Uploading a Language Pack will remove the existing one (if applicable) and will reboot the Quadro.

The **Current Language Pack** field displays read-only information about the custom language pack uploaded. When no custom language pack is uploaded, the field indicates "unknown".

Below, there is a **Language Pack File to Upload** text field that displays the selected image filename. The **Browse** button is used to browse the custom language pack to be uploaded.

The **Remove Current Language Pack** link is only seen when a custom language pack is uploaded and is also used to remove it from the system.

Pressing **Save** will start uploading the custom language pack to the board. The next page displayed will show verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if applicable).

After final confirmation, the system will upload the selected custom Language Pack and it will reboot.

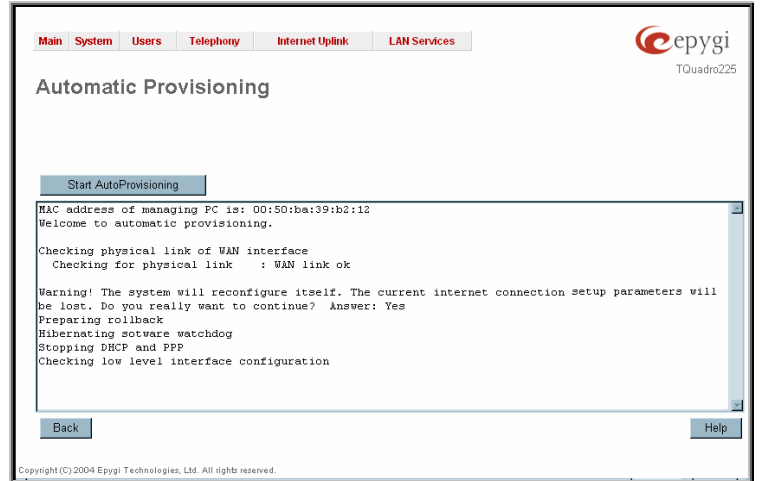


Fig. II-43: Auto Provisioning page

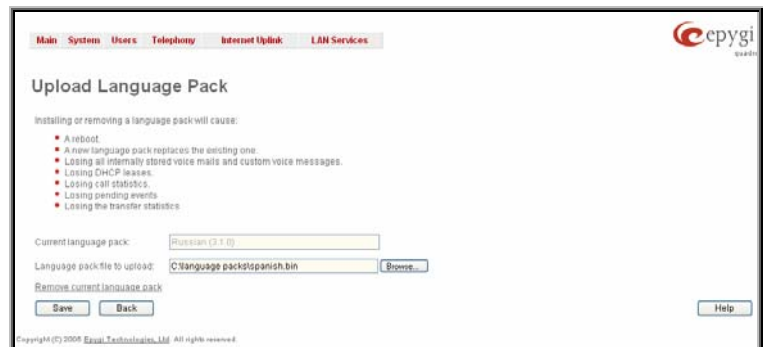


Fig. II-44: Upload Language Pack page

User Rights Management

The **User Rights Management** service sets restrictions on the GUI access for various users, permits or denies the access to certain Web GUI configuration pages and creates multilevel user management of the Quadro. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the Quadro's configuration.

Two levels of Quadro GUI administration are available:

- **Administrator** – this is the main administrator's account. The administrator can configure to have the factory reset safe the default password or choose not to. The administrator has access to all Web GUI pages and no one else has configuration permission to adjust this account. The administrator is responsible for granting access to all other user groups.
- **Local Administrator** – this is a common (sub-) administrator's account. The password is not factory reset safe. Local Administrator can have permission to adjust each GUI page.

The **User Rights Management** page consists of two pages. The **Users** page is used to manage the available users on the Quadro. The **Roles** page is used to assign the corresponding permissions to the users.

The **Users** page contains a table where the Administrator and Local Administrator users are listed. This page allows them to modify the passwords of available users in the table and to manage the Local Administrator's account. The following functional buttons are available on this page:

The **Change Password** functional button is used to change the password of the Administrator and Local Administrator user's account. Select one of the available users in the table by toggling the corresponding checkbox and press **Change Password** to open the corresponding page.

The **Change Password** page is used to change the user's password. It offers the following components:

The **Old Password** text field is only present when modifying the Administrator account password and requires the current password of the Administrator. An error message prevents entering the wrong password.

The **New Password** text field requires a new password for the Administrator or Local Administrator. Reentering the new password in the **Confirm New Password** text field will confirm the new password.

The password can consist of numerical values only. Up to 20 digits are allowed. A corresponding warning appears if any other symbols are inserted.

The **Store password in persistent area (Factory reset save)** checkbox is only present when modifying the Administrator's account password and is used to save the Administrator's password in the factory reset safe place.

Attention: Be EXTREMELY careful when enabling this checkbox. When it is done, the Administrator's password cannot be retrieved even after a factory reset. In this case, if the Administrator's password has been forgotten, the Quadro will be considered broken. Please contact Epygi Technical Support Center for replacing the device.

The **Enable User** and **Disabled User** functional buttons are used to enable or disable the Local Administrator's account.

Please Note: The Administrator's account cannot be disabled.

The **Roles** page contains a table where the Local Administrator and Extensions users are listed. This page allows you to set the permissions to the GUI pages for each user in the table.

The **Edit** functional button leads to the **Change Access Rights** page where a list of user specific GUI pages is displayed. Select the user in the table and press **Edit** to manage the permission for the corresponding user.

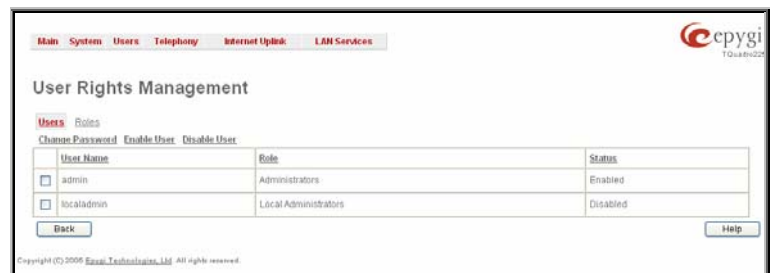


Fig. II-45: Users page at User Rights Management

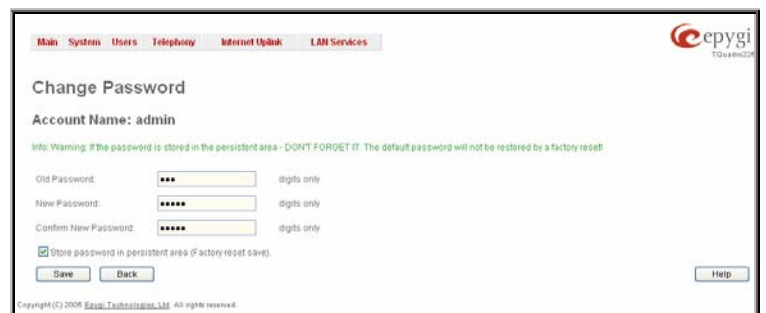


Fig. II-46: Change Password page



Fig. II-47: Roles page at User Rights Management

On the **Change Access Rights** page, **Grant Access/Deny Access** functional buttons are used to grant or deny access to certain GUI page(s) for the selected user.

When access to a certain GUI page is denied for a user, the "You are not authorized to access this page!" warning message will be displayed.

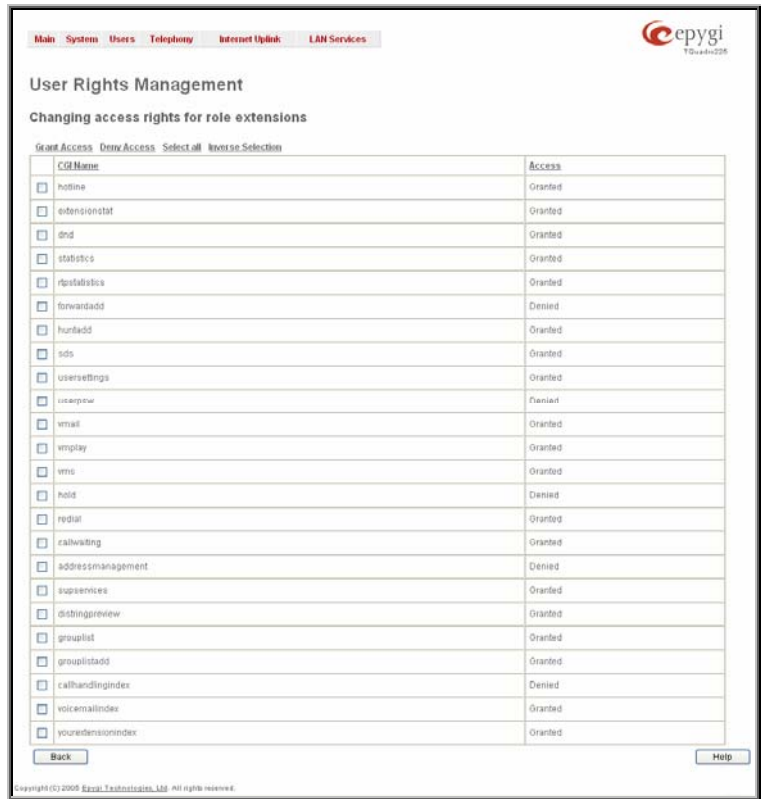


Fig. II-48: Edit Roles page at User Rights Management

Users Menu

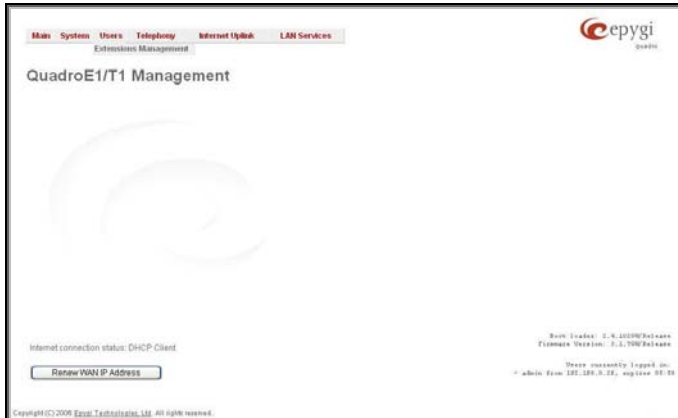
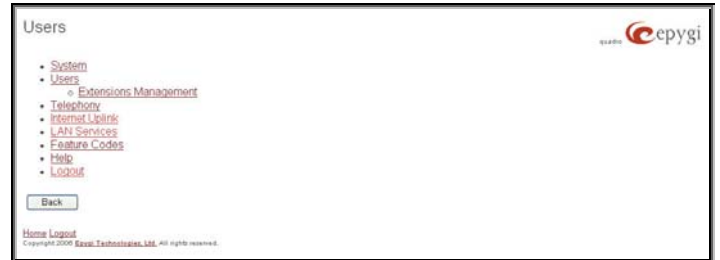


Fig. II-49: Telephone Users Menu in Dynamo Theme



F Fig. II-50: Telephone Users Menu in Plain Theme

Extensions Management

The **Extensions Management** is used to create user extensions and auto attendants on the Quadro. From this page, by clicking on the user extension, administrator can get the extension settings pages.

Two types of user extensions, **active** and **inactive**, can be created on the Quadro. Active extensions are those that are attached to a line, can place and receive calls and use available telephony services. Inactive extensions are those that are not attached to the line. They can use some available telephony services but they cannot place and receive calls. Instead, inactive extensions have a voice mailbox available to store the messages from callers.

QuadroE1/T1 has one available line and only one active extension can be configured.

Attendant extensions are dedicated to the IVR system on the Quadro. These extensions are used by callers to reach Quadro's users and use the remote access and call relay services. It is possible to create Auto Attendants with the custom scenarios. By default, Quadro has one Auto Attendant extension (00) which is undeletable.

The **Extensions** table is a list of all extensions and their parameters.

Extension	Display Name	Attached Line	SIP Address	H323 Address	Call Relay	Codecs
00	Attendant		79523200@sip.epygi.com:5060	00		PCMU...
<input type="checkbox"/> 77	GW-Attendant		77@sip.epygi.com:5060	77@h323.epygi.com:1719		PCMU...
<input type="checkbox"/> 11	GW User1	Line 1	79523211, Proxy:sip.epygi.com:5060	11@gk.epygi.com:1719	Yes (WARNING:password is empty)	PCMU...
<input type="checkbox"/> 56	GW User2	None	56@sip.epygi.com:5060	56@gk.epygi.loc:1719	Yes (WARNING:password is empty)	G726-32...
<input type="checkbox"/> 57	GW User3	None	57@sip.epygi.loc:5060	565441@gk.epygi.loc:1719	No	G726-32...

Fig. II-51: Extensions Management page

The following columns are present in the table:

- **Extension** - lists the 2-digit user or attendant extensions on the Quadro. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **Attached Line** - indicates the FXS or IP line corresponding extension it is attached to. "R" is displayed in this column when **SIP Remote Extension** (see below) functionality is enabled on the extension.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: "username, Proxy: sipserver:port". If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **H323 Address** - displays the H.323 address of the corresponding extension. Column displays the full H.323 address, (i.e., username@h323gatekeeper:port) when the **Registration on Gatekeeper** checkbox is selected. If registration is disabled, the Gatekeeper address will be displayed in the following format: "username, Proxy: h323gatekeeper:port". If no Gatekeeper Registration Address or

Gatekeeper Registration Port is defined, corresponding information will not be displayed in this column. If no username is defined, the extension number will be displayed instead.

- **Call Relay** - indicates whether or not the Call Relay option is enabled on the extension.
- **Codecs** – column lists the short information (full information is seen in the tool tip) about extension specific voice Codecs. Extension codec's can be accessed and modified by clicking on the link of the corresponding extension's Codecs. The link leads to the [Extension Codecs](#) page.

Clicking on each user extension in the Extensions table will open the extension specific **Extension Settings** menu. When Call Park service is enabled on the extension, it is displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible.

Add opens the **Add Entry** page where the type and number of the new extension should be defined. This page consists of the following components:

The **Extension** text field is used to enter a new extension number. The extension number is a two-digit number. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" will appear. If the extension length is shorter than 2 digits, the error "Incorrect Extensions length" will prevent the creation of the extension. If an extension with the same number already exists in the Extensions Management table, the error "Extension already exists" will appear.

Please Note: Each extension number cannot start with digits 0, 8 or 9.

The **Type** drop down list is used to select the type of the extension (user or attendant) to be created (for details see below).

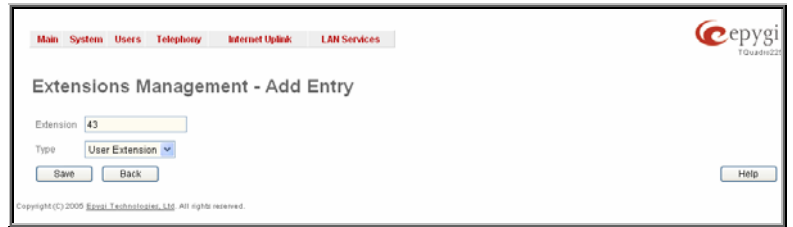


Fig. II-52: Extensions Management - Add Entry page

Edit opens the **Edit Entry** page where a newly created user or attendant extension settings might be adjusted. To operate with **Edit**, one or more record(s) have to be selected, otherwise the "No records selected" error message will appear.

The **Edit Entry** page consists of two frames. In the left frame settings groups are listed. Clicking on the corresponding settings group displays their configuration options in the right frame.

Please Note: Save changes before moving among settings groups.

1. General Settings

This group requires extension's personal information and has the following components:

Display Name is an optional parameter used to recognize the caller. Usually the display name appears on the called party's phone display when a call is made or a voice mail is sent.

Password requires a password for the new extension.

The extension password may only contain digits. If non-numeric symbols are entered, the "Incorrect Password: no symbol characters allowed" error will prevent making the extension.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the "Incorrect Password confirm" error will appear.

Attached Line lists all free lines to where an extension may be attached.

Please Note: Extensions cannot be detached from the line if the **SIP Remote Extension** service is enabled on it. To detach the extension from the line, disable the SIP Remote Extension service on the extension first.

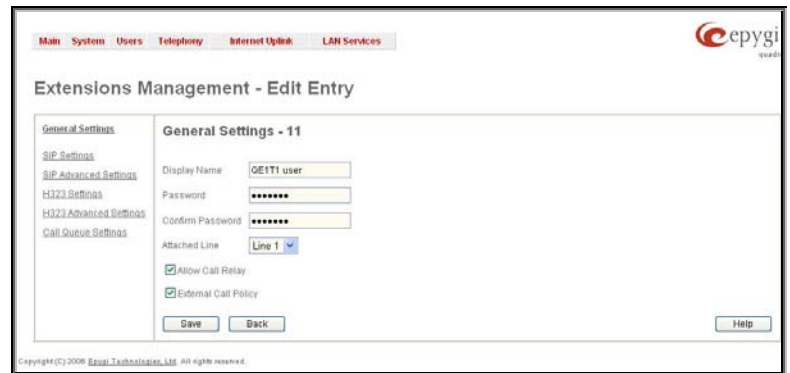


Fig. II-53: Extensions Management - Edit Entry – General Settings page

Allow Call Relay enables the current extension to be used to access the Call Relay service in the Quadro's Auto Attendant. It is recommended to define a proper and non-empty password when enabling this feature in order to protect the Call Relay service from an unauthenticated access.

When **External Call Policy** checkbox is enabled, all incoming IP calls to the corresponding extension will be handled by the external Policy Server.

2. SIP Settings

This group is used to configure extension's SIP registration settings and consists of the following components:

User Name requires a user name for the extension registration on the SIP server. The registration user name needs to be unique on the SIP server and it is displayed on the called phone when performing an IP call.

Password indicates the password for the extension registration on a SIP server.

Registration Password is used to confirm the password. If the entered password does not correspond to the one entered in the **Password** field, the error message "The passwords do not match. Please try again" will appear.

SIP Server indicates the host address of the SIP server. The field is not limited regarding symbol usage or length. It can be either an IP address such as 192.168.0.26 or a host address such as sip.epygi.com.

Registration SIP Port indicates the host port number to connect to the SIP server. The SIP server port may only contain digit values, otherwise the error message "SIP Server Port is incorrect" will be displayed when applying the extension settings. If the SIP server port is not specified, Quadro will access the SIP server through the default port 5060.

Registration on SIP Server enables the SIP server registration option. If the extension has already been registered on an SIP server, its IP address will be displayed in brackets.

3. SIP Advanced Settings

This group is used to configure advanced SIP settings (Outbound Proxy, Secondary SIP Server and Outbound Proxy for the Secondary SIP Server settings and to define other SIP server specific settings).

The SIP Outbound proxy is an SIP server where all the SIP requests and other SIP messages are transferred. Some SIP servers use an outbound proxy server to escape restrictions of NAT. For example, Free World Dialup service uses an Outbound Proxy server. If an Outbound proxy is specified for an extension, all SIP calls originating from that extension are made through that outbound proxy, i.e., all requests are sent to that outbound proxy, even those made by Speed Calling.

The Secondary SIP Server acts as an alternative SIP registration server when the primary SIP Registration Server is inaccessible. If the connection with the primary SIP server fails, Quadro will automatically start sending SIP messages to the Secondary SIP Server. It will switch back to the primary SIP server as soon as the connection is reestablished.

Authentication User Name requires an identification parameter to reach the SIP server. It should be provided by the SIP service provider and can be requested for some SIP servers only. For others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism.

Timeout indicates the timeout between two attempts for the SIP registration server accessibility verification. If no reply is received from the primary SIP server within this timeout, the Secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will resume being sent to it.

The **RTP Priority Level** drop down list is used to select the priority (low, medium or high) of the RTP packets sent from a corresponding extension. RTP packets with higher priority will be sent first in case of heavy traffic.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name) and the port numbers of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

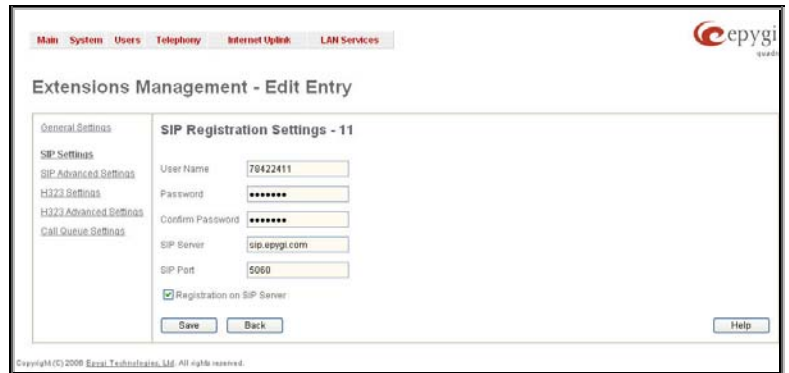


Fig. II-54: Extensions Management - Edit Entry – SIP Settings page

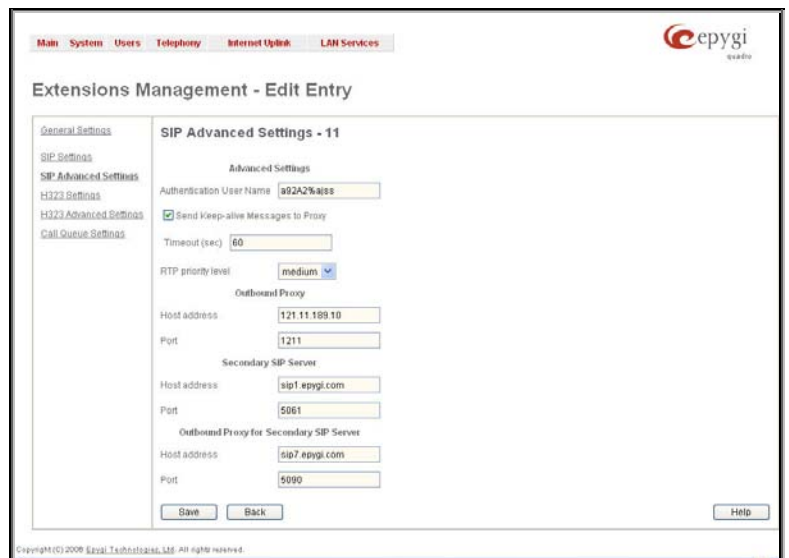


Fig. II-55: Extensions Management - Edit Entry – Advanced SIP Settings page

4. H323 Settings

This group is used to configure the extension's H.323 registration settings and consists of the following components:

Enable H323 checkbox enables H323 protocol support on the extension. If this feature is enabled, corresponding extension is free to accept and place H323 IP calls.

Registration User Name Type drop down list is used to choose the type of the H323 registration user name: e164, H323ID, URL or Email.

Registration User Name requires a user name for the extension registration on the H323 gatekeeper. Depending on the **H323 Registration User Name Type** selected in the list above, **Registration User Name** inserted in this field may contain different characters: for **e164** user name type digit characters allowed only, **H323ID** user name type allows any characters for the registration user name, **URL** registration user name requires IP address or the hostname, while **Email** registration user name requires an email address. The registration user name needs to be unique on the H323 gatekeeper and is being displayed on the called phone whenever performing an IP call.

Registration Password indicates the password for the extension registration on a H323 gatekeeper.

Confirm Registration Password is used to confirm the password. If the entered Password does not correspond to the one given in the **Registration Password** field, the error will appear: "The passwords do not match. Please try again".

Gatekeeper Registration Address indicates the host address of the H323 gatekeeper. The field is not limited regarding symbol usage and length as it can be either an IP address (ex: 192.168.0.26) or a host address (ex: h323.epygi.com).

Gatekeeper Registration Port indicates the host port number to connect to the H323 gatekeeper. The H323 gatekeeper port may only contain digit values, otherwise the error message "H323 gatekeeper Port is incorrect" will be displayed when applying the extension settings. If the Gatekeeper Registration Port is not specified, Quadro will access the H323 gatekeeper through the default port 1719.

Registration on Gatekeeper enables the H323 gatekeeper registration option. If the extension has already been registered at some H323 gatekeeper its IP address will be displayed in brackets.

5. H323 Advanced Settings

The **H323 Advances Settings** page is used for the H.323 gateway settings configuration to allow Quadro extension to use services provided by the H.323 gateway. Depending on the H.323 gateway configuration, it can provide call routing services to the different type of networks (e.g. PSTN).

The **UserID** (Alias Name) text field requires an identification parameter to reach the H323 Gatekeeper. It should be provided by the H323 service provider and can be requested for some H323 Gatekeepers only, for others field should be left empty.

The **Address** text field requires the IP address or the host name of the H.323 gateway. The **Port** text field requires the port number of the H323 gateway.

The **Dial Access Plan** text field requires a service identification number H323 gateway provides to the extension. This option is independent from the **Address** and **Port** parameters, i.e. can be also configured when other two fields are empty.

Address, **Port** and the **Dial Access Plan** are provided by the H.323 service provider and are used by Quadro to set the H.323 gateway specific features.

Please Note: **Address** and **Port** settings specified here will be only used when extension is not registered on the H.323 gatekeeper (and will be ignored in the contrary case), also when originating the H.323 IP call using shared H.323 registration settings of this extension.

6. Call Queue Settings

This group is used to configure the **Call Queue** service that allows multiple incoming calls to be kept in the queue when being on the line and enables the calls to be answered in the order they have been received.

Fig. II-56: Extensions Management - Edit Entry – SIP Settings page

Fig. II-57: Extensions Management - Edit Entry – Advanced SIP Settings page

The **Enable** checkbox activates the Call Queue functionality on the extension.

The **Call Queue Size** text field requires the length of the call queue. This is the maximum number of calls that will be accepted into the queue and kept on hold while the extension user is on a call. If a maximum number of calls are already held in the call queue, the next incoming call will be disconnected.

Please Note: By configuring Call Queue size, Call Forwarding if Busy and Voice Mail telephony services will not take effect on the corresponding extension until the call queue is not filled. These telephony services will affect only the calls out of the call queue.

The **Max Call Queue Appearance** text field requires the maximum number of active calls on the line. For example, if 1 is configured in this field and the extension is in use, the next incoming call will go to the call queue. If 2 is configured in this field and extension is in use, the next incoming call alert will be heard in the background (if Call Waiting service is enabled on the corresponding extension) and the extension will hold the first call to answer the second one or they can be joined for a call conference. However, the next incoming call will again go to the call queue.

Upload new call queue welcome message allows updating the active Call Queue welcome message (played when a caller joins the extension's call queue), downloading it to the PC, or restoring the default one.

The **Remove call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue welcome message** functional link appears only when the custom call queue welcome message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Upload new call queue message allows updating the active call queue message (played when a caller is being held in the queue), downloading it to the PC, or restoring the default one.

The **Remove call queue message** functional link appears only when the custom call queue message is already uploaded and is used to remove it and restore the default call queue welcome message.

The **Download call queue message** functional link appears only when the custom call queue message is already uploaded and is used to download it to PC and opens the file chooser window where the saving location can be specified.

Browse buttons open the file chooser window to browse for a new Call Queue welcome message file. The uploaded files should be in PCMU wave format, otherwise the system will prevent uploading it with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading if there is not enough memory available for the corresponding extension, which will cause the "You do not have enough space" warning message.

For **Attendant** extensions, the **Extensions Management - Edit Entry** page consists of **General Settings**, **Attendant Scenario**, **SIP Settings**, **SIP Advanced Settings**, **H323 Settings**, **SIP Advanced Settings** pages. The **SIP Settings** and **SIP Advanced Settings** pages are the same as for the regular extensions described above. The **General Settings** and **Attendant Scenario** pages are described below:

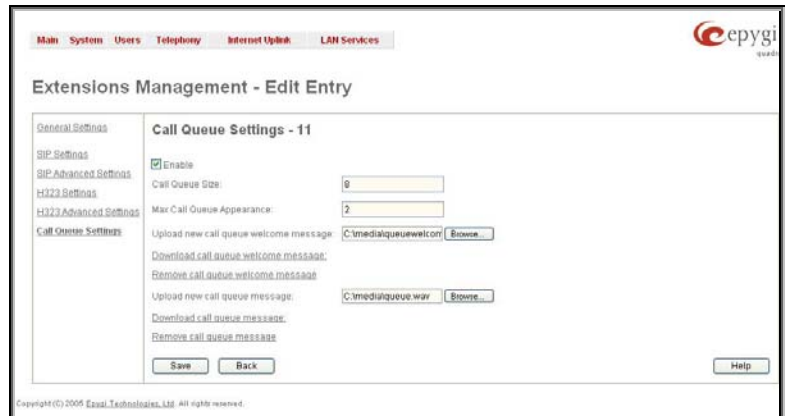


Fig. II-58: Extensions Management - Edit Entry – Call Queue Settings page

1. General Settings (for attendant extension)

This group requires personal extension information and has the following components:

Display Name is an optional parameter used to define the Auto Attendant's description. Usually the display name appears on the called party's phone display when a call is made or a voice mail is sent.



Fig. II-59: Extensions Management - Edit Entry – General Settings for Auto Attendant page

2. Attendant Scenario

This group is used to select between default and custom attendant functionality scenarios. When the **Default** scenario is selected, a group of settings should be adjusted. The user defined Auto Attendant welcome messages can be uploaded and the list of **Friendly Phones** can be configured. For **Custom** scenario, a scenario script file (in EpygiXML coding, the coding standard can be found at [Epygi Technical Support](#)) should be defined and the custom voice messages can be uploaded.

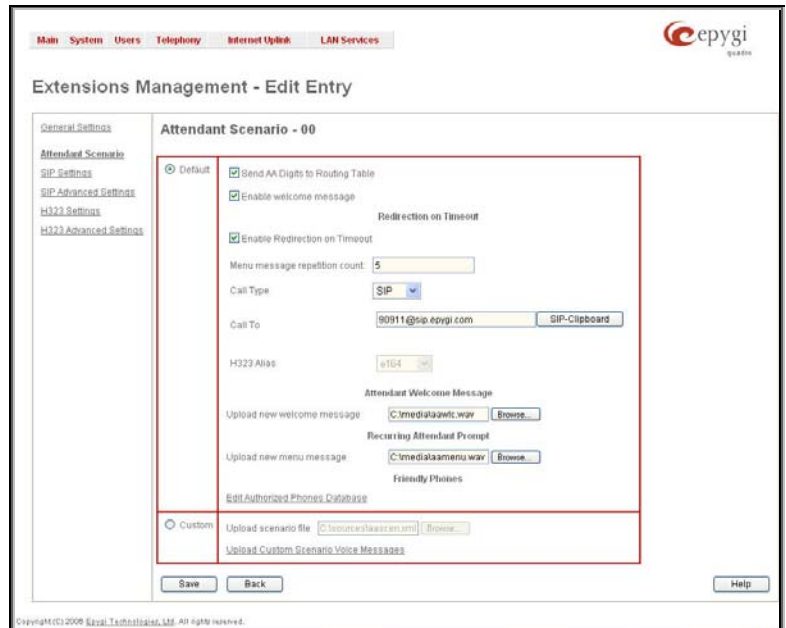


Fig. II-60: Extensions Management - Edit Entry – Attendant Scenario page

The **Default** manipulation radio button selection enables following components:

- The **Send AA Digits to Routing Table** checkbox selection switches the Auto Attendant to the routing mode. Any inserted digits in Auto Attendant prompt will be parsed through the Routing Table on the Quadro.
- **Enable Welcome Message** checkbox is used to enable/disable the Auto Attendant welcome message (the default one or the custom one uploaded from this page or recorded from the handset (see Feature Codes) being played when callers enter Quadro's Auto Attendant.
- **Redirection on Timeout** - this group allows automatic call redirection in case if no actions has been performed by the caller. The group offers the following options:

Enable Redirection on Timeout checkbox is used to enable/disable the automatic call redirection.

Menu Message Repetition Count text field indicates the number of Auto Attendant menu messages to be consecutively played to the caller with no action from his/her side. When the menu message is played the number of times indicated in this text field, the call will be automatically redirected to the defined destination.

Call Type drop down list includes possible incoming call types (PBX, PSTN, SIP, H323 or Auto). PBX selection means that the call will be redirected to the local extension. **SIP** or **H323** selections mean that the call will be redirected to the SIP or H.323 destination correspondingly. **PSTN** selection means that the call will be redirected to the PSTN destination. **Auto** selection is used for undefined call types: destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

Call To text field requires the destination number dialed in the format depending on the selected Call Type. The wildcard is supported in this field.

H323 Alias field is actual for H323 call type only and may contain different characters: for **e164** user name type digit characters allowed only, **h323-ID** user name type allows any characters for the registration user name.

- **Attendant Welcome Message** - this group allows updating the active Auto Attendant welcome message (played only once when entering Auto Attendant), downloading it to the PC, or restoring the default one. The group offers the following components:

The **Restore Default Welcome Message** checkbox allows restoring the Auto Attendant default welcome message file if another one has been previously selected. If the checkbox is selected, the file upload will be disabled.

Upload new welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCM-U wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.

Browse opens the file chooser window to browse for a new welcome message file.

The **Download Welcome Message** and **Remove Welcome Message** links appear only if a file has been uploaded previously. The **Download Welcome Message** link is used to download the message file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Welcome Message** link is used to restore the default welcome message.

- **Recurring Attendant Prompt** - this group allows updating the active recurring Auto Attendant message (played after the Attendant Welcome Message and then periodically repeated while being in the Auto Attendant), downloading it to the PC, or restoring the default one. The group offers the following components:

The **Restore Default Recurring Attendant Prompt** checkbox allows restoring the Recurring Attendant Prompt file if another one has been previously selected. If the checkbox is selected, the file upload will be disabled.

Upload new Recurring Attendant Prompt indicates the file name used to upload a new recurring auto attendant prompt. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning message to appear.

Browse opens the file chooser window to browse for a new menu message file.

The **Download Welcome Message** and **Remove Welcome Message** links appear only if a file has been uploaded previously. The **Download Welcome Message** link is used to download the message file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Welcome Message** link is used to restore the default welcome message.

- **Friendly Phones** - the **Edit Authorized Phones Database** link refers to the [Authorized Phones Database](#) page where a list of trusted external phones can be created. If external SIP or PSTN users are added to the Quadro Authorized Phones database, they are free to access the Auto Attendant Services without passing the authentication or to use the Call Back services.

The **Custom** manipulation radio button selection allows you to upload Attendant's custom scenario file and voice messages. The selections are:

- The **Upload Scenario File** indicates the file name used to upload a new scenario file. The uploaded file needs to be in EpygiXML format (the coding standard can be found at [Epygi Technical Support](#)) and is restricted to a 20KB file size. **Browse** opens the file chooser window to browse for a custom scenario file.
- The **View/Download Scenario** link appears only when a custom scenario file has been previously uploaded and is used to view or download the scenario file. The **Remove Scenario** link is used to remove a custom scenario file and return to the default Auto Attendant scenario.
- The **Upload Custom Scenario Voice Messages** link refers to the page where voice messages used in the uploaded custom scenario should be managed.

This page provides the possibility of uploading voice messages to be played in the custom Auto Attendant scenario. It also removes and downloads the uploaded files to a PC.

The **Upload Custom Scenario Voice Messages** page contains a table where uploaded custom voice messages are listed. Use the **Download** functional button to download and use **Remove** to delete the corresponding custom voice message. **Browse** opens a file chooser window to browse for a custom voice message.



Fig. II-61: Upload Custom Voice Messages page

The **Edit** functional button provides a possibility of editing multiple extensions at the time. In this case, fields that cannot be edited for multiple records have **Multiple** values in the **Edit Entry** page. When editing user and attendant extensions together, **Edit Entry** page displayed only those fields that are general for both user extension and attendant settings. Additionally, for the fields that need to be modified, a **Select to modify fields** checkbox alongside the corresponding field needs to be selected to submit changes, otherwise the fields will not be updated.

Delete removes the selected extensions. If no records are selected an error message occurs.

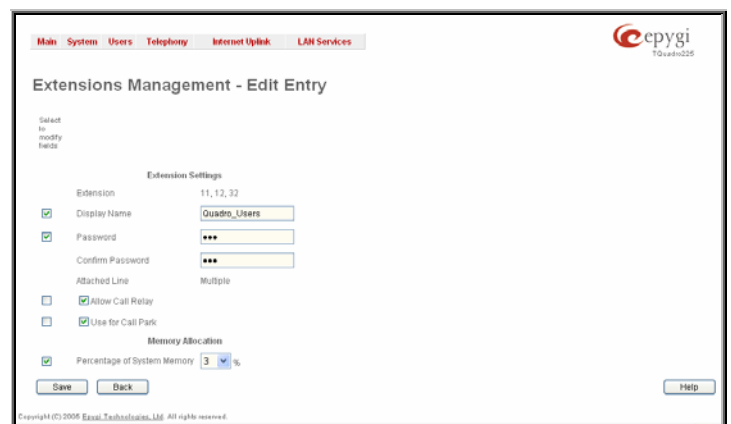


Fig. II-62: Extensions Management - Edit Entry page for multiple edit operation

To Configure an Extension

1. Press the **Add** button on the **Extensions Management** page. The **Add Entry** page will appear in the browser window.
2. Enter the desired extension number in the **Extension** text field and select the extension type from the **Type** drop down list.
3. Press **Save** to create an extension with the defined number.
4. Select the checkbox of the newly created extension in the **Extensions Management** table and press the **Edit** button. The **Edit Entry** page will appear in the browser window.
5. Move through the extension's configuration pages and fill the fields with the appropriate information.
6. To apply extension settings, press **Save**.

To Delete an Extension

1. To remove an extension with all its settings select one or more checkboxes of the corresponding extensions that should be deleted from the **Extensions Management** table. Press **Select all** if all extensions should be deleted.
2. Click on the **Delete** button on the **Extensions Management** page.
3. Confirm the deletion by clicking on **Yes**. The extension(s) will be deleted. To abort the deletion and keep the extension in the list, click **No**.

Extension Codecs

To establish IP voice communication, both partners have to use the same codec. When establishing the communication line, this codec is negotiated. If the caller does not find an appropriate codec, the communication cannot take place. If you want to be reachable by all IP calls, it is helpful to support as many codecs as possible. In this case, all the codecs that Quadro offers should be added to the **Active Codecs** table. Some codecs require a high transfer rate of up to 64 kbit/s. If you are certain you do not want to use these codecs, make sure they are not listed in the table **Active Codecs**.

The **Extension Codecs** page displays a list of **Active Codecs** with the state of the **Out of Band DTMF** and **FAX Support** features for Quadro extensions and the Auto Attendant.

Please Note: Use caution when configuring Auto Attendant Codecs as they are used by virtual extensions for redirecting the incoming calls.

The table **Active Codecs** lists active voice codecs for the selected line that are supported by Quadro. The order of records in the **Active Codecs** table is important for transmitting and receiving. A codec placed at the top of the table will be used as the preferred codec. If the remote party does not support the preferred codec, the following codecs will be tried in a top to down order in the **Active Codecs** table.

Each record in the table has an assigned checkbox. They are used to select the record to be deleted or moved up or down.

An error occurs if no records are selected and the user activates the delete button, the "No records selected" error message appears. At least one codec must be attached to the line. When attempting to delete the last codec, the "At least one codec should stay in the codec list" error message will appear.

Add opens the **Add Entry** page where the user may add codecs supported by Quadro. The voice codec defines the voice compression algorithm for the incoming and outgoing DSP packages.

Codecs lists all codecs supported by Quadro. If no more codecs are available (all available codecs have already been transferred to the **Active Codecs** table), the **Add Entry** page will display the message "No Available Codecs" instead of the drop down menu.

The **Move Up/Move Down** buttons are used to move the selected codec one level up/down in the table.

The **Out of Band DTMF Transport** checkbox enables DTMF code transmission in parallel with the voice stream. The destination receiving the DTMF code will play it locally if it supports the feature. This is helpful to avoid DTMF's loss upon bad traffic. This feature is valuable for all codecs but it is especially recommended to enable it in case low bit rate codecs (G729, G723, G726/16, etc.) are selected.

Enable T.38 FAX checkbox enables the FAX tone detection and the T.38 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line. **Enable Pass Through FAX** checkbox enables the FAX tone detection and the G711 codec support for the FAX transmission from/to the Fax Machine/Fax modem attached to the line.

If both of these checkboxes are enabled, T.38 codec will be used as preferred codec for FAX transmit/receive and if not acceptable by the peer, G711 codec will be used instead.

Please Note: If both of these checkboxes are disabled, no FAX transmission to the peer's voice mailbox will be possible. Checkboxes are applicable for FAX transmission/receipt over an IP network only.

Enable Pass Through Modem checkbox enables the modem tone detection and the G711 codec support for the data transmission from/to the modem attached to the line. During data transmission, Silence Suppression (see [RTP Settings](#)) and Echo Cancellation are being disabled on the line.

The **Force Self Codecs Preference for Inbound Calls** checkbox enables the usage of your own preferred codecs (if available on both peers) for the IP connection establishment on the extension.

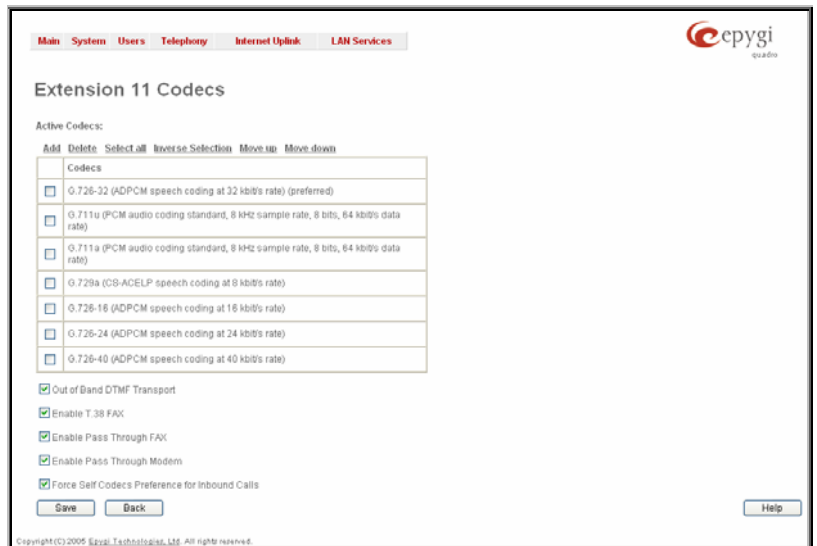


Fig. II-63: Extension Codecs list

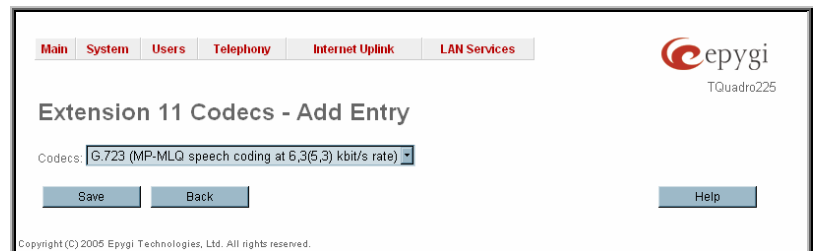


Fig. II-64: Extension Codecs - Add Codec page

Authorized Phones Database

The **Authorized Phones Database** page is used to create a list of trusted external phones. If they are part of the Quadro Authorized Phones database, external SIP or PSTN, then users are free to access the Quadro Auto Attendant services without requiring authentication. When adding a trusted phone to the list, an existing extension has to be chosen. The parameters (extension number and password, as well as SIP and Speed Calling Settings) will be used automatically for the trusted caller access of the Quadro Auto Attendant. A direct connection to the **Call Relay** menu can be optionally provided.

The **Authorized Phones Database** page displays the **Authorized Phones Database** table where the trusted phones are listed. Only SIP and PSTN users can be added to the **Authorized Phones Database**.

The **Authorized Phones Database** table displays all trusted callers with their settings. For example, the call type, caller address, extension they automatically login with, information if they have automatic access to Call Relay Menu of the Auto Attendant, etc.

Each record in the table has an assigned checkbox. The checkbox is used to edit or delete the corresponding record. The "No records selected" error message occurs if the user activates the edit or delete button with no records being selected. The error message "One record should be selected" appears if the user tries to edit more than one record. The heading of each column in the table has a link. By clicking on the column heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The **Add** functional button refers to the **Authorized Phones Database- Add Entry** page where new trusted users may be entered.

The **Authorized Phones Database- Add Entry** page offers two group of input options:

Caller Settings

The **Call Type** drop down list includes possible incoming call types (PSTN, SIP or Auto). In **SIP**, the caller connects Quadro through a SIP server and **PSTN** means the caller is a PSTN user. **Auto** is used for undefined call types and the destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

The **Caller Address** text field requires the caller's SIP address (see chapter [Entering a SIP Addresses correctly](#)) or PSTN number to be added to the trusted phones list. The PSTN number length depends on the area code and phone number. The wildcard is supported in this field. If the caller address already exists in the **Authorized Phones Database**, the error message "The record already exists" appears when selecting the **Save** button.

H323 Alias field is actual for H323 call type only and may contain different characters: for **e164** user name type digit characters allowed only, **h323-ID** user name type allows any characters for the registration user name.

The **Login Extension** drop down list provides all existing extensions on the Quadro. When calling the Quadro Auto Attendant, a trusted user will automatically login with the selected extension, i.e., extension number and its password will be automatically submitted by the Quadro system. The trusted user will directly access the Quadro Auto Attendant services. The SIP settings of login extension will be used while making IP calls.

The **Automatically Enter Call Relay Menu** checkbox enables direct access for the trusted user to the Quadro Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but will still be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

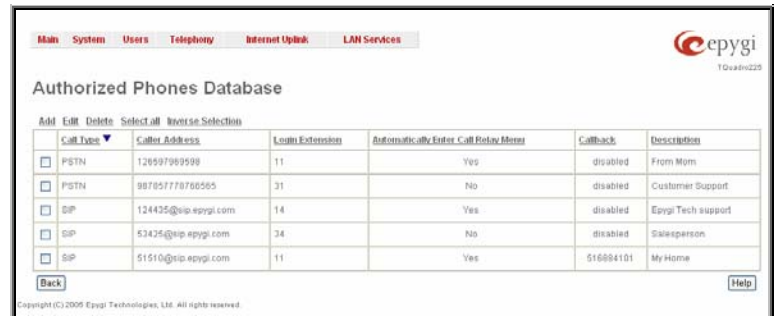
The **Description** text field allows entering an optional comment.

To Add an Authorized phone to the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. Press the **Add** button on the **Authorized Phones Database** page. The **Add Entry** page will appear in the browser window.
4. Choose the call type and enter a caller address in the corresponding text field.
5. Select a **Login Extension** and the **Automatically Enter Call Relay Menu** checkbox (if required).
6. Fill in an optional **Description** in the appropriate field, if required.
7. Press **Save** to submit the settings.

To Delete an Authorized phone from the database

1. Enter the desired **Auto Attendant Settings** page.
2. Select **Edit Authorized Phones Database** to enter the **Authorized Phones Database** page.
3. To remove an authorized phone(s), select one or more checkboxes of the corresponding records that should be deleted from the **Authorized Phones Database** table. Press **Select all** if all records should be deleted.
4. Press the **Delete** button on the **Authorized Phones Database** page.
5. Confirm the deletion by clicking on **Yes** or cancel the action by clicking on **No**.



Call Type	Caller Address	Login Extension	Automatically Enter Call Relay Menu	Callback	Description
PSTN	1299799999	11	Yes	disabled	From Mom
PSTN	98765778766565	31	No	disabled	Customer Support
SIP	124435@ip.epygi.com	14	Yes	disabled	Epygi Tech support
SIP	53425@ip.epygi.com	34	No	disabled	Salesperson
SIP	51510@ip.epygi.com	11	Yes	\$16884101	My Home

Fig. II-65: Authorized Phones Database

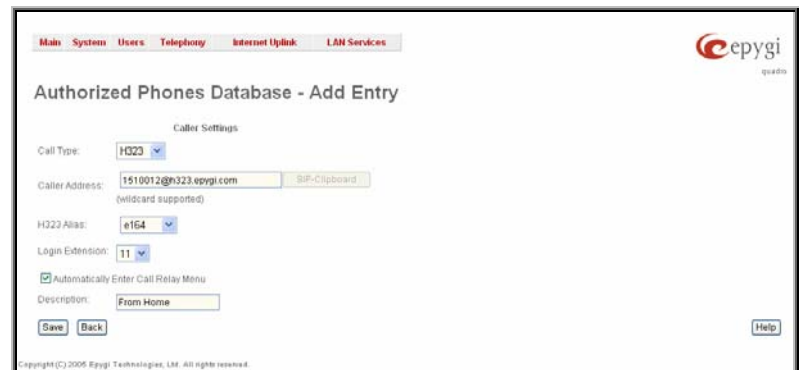


Fig. II-66: Authorized Phones Database - Add Entry page

Telephony Menu

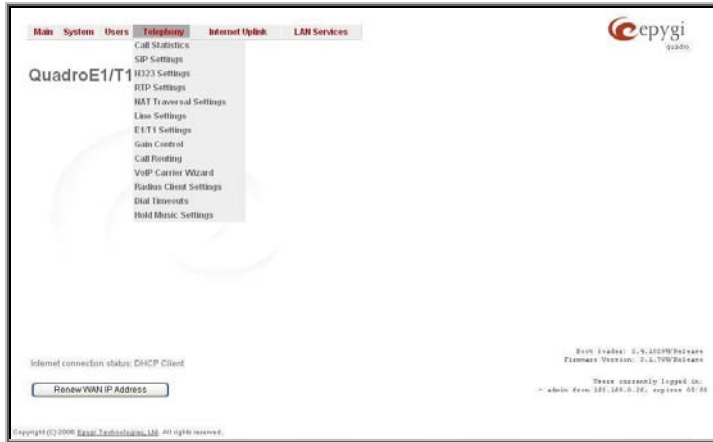


Fig. II-67: Telephony Menu in Dynamo Theme



Fig. II-68: Telephony Menu in Plain Theme

Call Statistics

The **Call Statistics** page displays four tables. They provide information on successful, unsuccessful and missed incoming and outgoing calls on the first three tables, and statistics settings on the fourth page. Call statistics allows the collecting of call events on the Quadro with their parameters and to search them by various criteria.

The **Statistics Settings** page offers the following input options:

The **Enable Call Reporting** checkbox enables Call Statistics reporting. The selected number of statistics entries will be displayed in the Call Statistics tables.

The **Maximal Number of Displayed Call Records** drop down lists are used to select the number of **Successful**, **Missed** and **Nonsuccessful** statistics entries to be displayed in the corresponding **Call Statistics** tables. If the record numbers exceed the numbers specified in these drop down lists, the oldest record will be removed.

The **Download Call Statistics** link is used to download all displayed statistics in a file that can be viewed with a simple text editor.

The **Clear all Records** button is used to clear all statistics records.

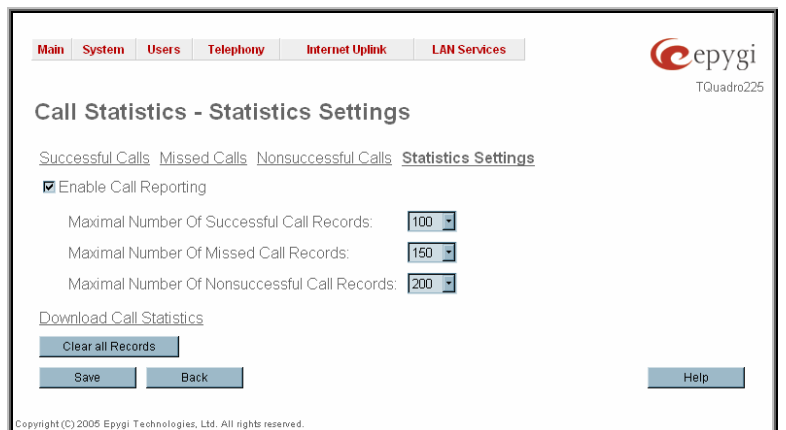


Fig. II-69: Call Statistics Settings page

The **Number of Records** displays the current number of statistics entries in the table. For successful calls, **Total Duration**, **Maximum Duration**, **Average Duration** and **Minimum Duration** statistics are displayed on top of the table.

The **Call Statistics: Successful Calls**, **Missed Calls** and **Nonsuccessful Calls** pages consist of the general information on successful, missed and unsuccessful calls, search fields and the calls table. The search components are as follows:

From and **To** text fields are used to search by date and time. The data must be entered in either of the following formats: dd-mm-yyyy hh:mm:ss or dd-Mon-yyyy hh:mm:ss. The time criteria are optional. **From** requires an earlier date and time than the **To** field. If the entered data does not meet this condition, the error message "Minimal date should be less than maximal date" prevents statistics filtering.

From and **To** drop down lists are used to search by duration. The duration has to be selected from the list of values. **From** field must indicate a shorter duration than the **To** field. If the inserted data does not meet this condition, the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.

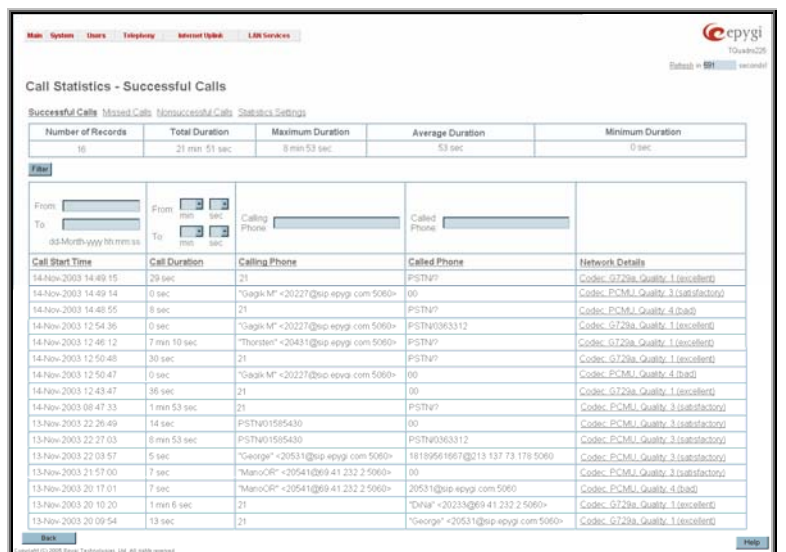


Fig. II-70: Call Statistics page

Calling Phone and **Called Phone** respectively require the caller and called party's SIP address (see chapter [Entering a SIP Addresses correctly](#)), extension or PSTN number as search criteria. Wildcard symbols are allowed here.

The **Call Statistics: Successful Calls, Missed Calls and NonSuccessful Calls** tables are lists of successful, missed and unsuccessful incoming and outgoing calls and their parameters (Call Start Time, Call Duration, Call destinations). Each column heading in the tables is a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will be displayed close to the column heading.

The **Network Details** column is only present in the **Successful Calls** table and provides brief information about the call quality and codecs used to receive and transmit packets. Clicking on the successful call details will open the [RTP Statistics](#) page where detailed information about the established call is provided. The **Call Detail** column is present only in the **Non Successful Calls** table and indicates the reason why the call was unsuccessful.

Filter performs a search procedure by the selected criteria. The search may be done with several criteria at the same time.

To Enable/Disable the Statistics

1. Enter the **Call Statistics Settings** page.
2. Select or deselect the **Enable Call Reporting** checkbox to enable or disable statistics recording.
3. If enabling the statistics, the maximum number of records to be stored in the statistics table should be selected from the corresponding drop down lists.
4. Press **Save** to apply the new configuration.

To Filter the Statistics

1. Enter the desired criteria fields.
 2. Press the **Filter** button to search the call reports within the **Call Statistics** table.
- Please Note:** To return to the complete **Statistics Table**, clear all search criteria and press **Filter**.

To Reset the Statistics

1. Press the **Clear All Records** button in the **Call Statistics Settings** page.
2. Confirm the deletion by clicking on **Yes**. The call statistics will then be deleted. To abort the deletion and keep the statistics information, click on **No**.

RTP Statistics

The **RTP Statistics** page provides detailed information about the established call is provided.

Quality - estimated call quality, which depends on RTP statistic. Below is the legend for Call Quality definitions on the displayed RTP Statistics:

- excellent** – RX Lost Packets < 1% & RX Jitter < 20
- good** - RX Lost Packets < 5% & RX Jitter < 80
- satisfactory** - RX Lost Packets < 10% & RX Jitter < 150
- bad** - RX Lost Packets < 20% & RX Jitter < 200
- very bad** - RX Lost Packets > 20% or RX Jitter > 200

- Rx/Tx Codec** - codec for received and transmitted RTP stream respectively.
- Rx/Tx Packets** - number of RTP packets received and transmitted respectively.
- Rx/Tx Packet Size** - size of RTP packet (payload) received and transmitted respectively.
- Rx Lost Packets** - number of lost RTP packets for received stream.

Rx Jitter - inter-arrival jitter is an estimate of the statistical variance of the RTP data packet inter-arrival time, measured in timestamp units. The inter-arrival jitter is defined to be the mean deviation (smoothed absolute value) of the difference D in packet spacing at the receiver compared to the sender for a pair of packets. If Si is the RTP timestamp from packet i, and Ri is the time of arrival in RTP timestamp units for packet i, then for two packets i and j, D may be expressed as:

$$D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si)$$

$$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16, \text{ where } J(i) \text{ is Rx Jitter for packet } i.$$

For more details about Jitter calculations, please refer to the RFC1889.

Rx Maximum Delay - maximum variance (absolute value) of actual arrival time of the RTP data packet compared to estimated arrival time, measured in milliseconds.

If Si is the RTP timestamp from packet i, and Ri is the time of arrival in RTP timestamp units for packet i, then variance for packet i may be expressed as following: $V(i) = |(Ri - R1) - (Si - S1)| = |(Ri - Si) - (R1 - S1)|$

$$\text{Rx Maximum Delay} = \max V(i) / 8$$

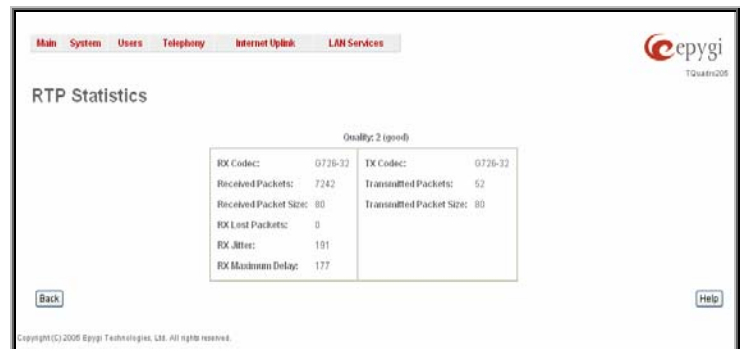


Fig. II-71: RTP Statistics page

Please Note: RTP Statistics is logged only when at least one of the call endpoints is located on the Quadro. For example, it will not be logged when:

- calls incoming from or addressed to the IP lines or remote extension,
- calls from an external user are routed to another external user through Quadro's routing rules.

In the first case, RTP statistics will be logged if remote extension or IP line user is calling locally to the Quadro's extension or auto attendant.

SIP Settings

The **SIP Settings** provide information on the SIP receive UDP and TCP ports and allows you to select DNS server configurations for SIP and the SIP timers scheme.

The **UDP Port** indicates the SIP UDP (User Datagram Protocol) receive port number. By default 5060 is selected and used. The SIP UDP port cannot be in the selected RTP/RTCP port range for FXS and IP lines (see [RTP Settings](#)), otherwise the "Mapped port for SIP shouldn't be in RTP port range" error message appears.

The **TCP Port** indicates the SIP TCP (Transmission Control Protocol) receive port number. By default 5060 is selected and used.

Please Note: Quadro will not use TCP protocol as a transport for SIP messages if the **TCP Port** field is left empty.

Enable Session Timer enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.

The screenshot shows the 'SIP Settings' page. At the top, there are navigation tabs: Main, System, Users, Telephony, Internet Uplink, and LAN Services. The 'SIP Settings' title is followed by the Epygi logo and 'TQuadro225'. The main content area includes:

- UDP Port: 5060
- TCP Port: 5060
- Enable Session Timer
- DNS server for SIP:
 - Use default: Use the DNS defined in the network settings
 - Specific:
 - SIP DNS 1: 192.168.77.19 IP-Clipboard
 - SIP DNS 2: 10.20.30.10 IP-Clipboard
- SIP timers:
 - RFC3261: All timers according to the standard
 - High availability: The retry periods are shortened
 - Custom: All timers according to the standard, except:
 - Registration timeout: 1800 second(s)
 - Registration failure timeout: 120 second(s)
 - Transaction duration: 32 second(s)
 - Session refresh timeout: 1800 second(s)

 At the bottom, there are 'Save', 'Back', and 'Help' buttons. A copyright notice at the very bottom reads: Copyright (C) 2005 Epygi Technologies, Ltd. All rights reserved.

Fig. II-72: SIP Settings page

The **DNS server for SIP** radio button group allows you to choose between regular DNS servers configured in the [DNS Settings](#) page and specific DNS servers for SIP traffic.

- **Use default** is used to apply regular DNS servers for SIP traffic.
- **Specific** is used to enable SIP specific DNS servers. For this selection, both primary and secondary SIP DNS servers should be defined in the **SIP DNS 1** and **SIP DNS 2** text fields. At the least, a primary DNS server should be inserted.

The **SIP Timers** radio button group is used to define the timeouts of the SIP messages retransmission.

- **RFC 3261** will apply standard SIP timers described in the corresponding specification.
- **High availability** will apply SIP timers to shorten the call establishment, registration confirmation and registration failure procedures. This selection provides more firmness to the SIP connection but increases the network traffic on the Quadro.
- **Custom** allows manually defining the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session refresh timeout** SIP timers (in seconds).

H323 Settings

The **H323 Settings** provide information on the H.225 RAS receive UDP port and H.323 TCP port range, enable H323 specific options as well as allows to enable the NAT traversal for the H.323 traffic.

The text field **UDP Port** indicates the H.225 RAS UDP (User Datagram Protocol) receive port number. UDP port cannot be in the selected RTP/RTCP port range for FXS and IP lines (see [RTP Settings](#)) otherwise error appears.

The text fields **TCP Min Port** and **TCP Max Port** text fields are used to indicate the TCP (Transmission Control Protocol) receive port range for H.225 call signaling and H.245 media negotiation. The port defined in the **TCP Min Port** text field will be used for accepting the incoming direct H.323 calls.

There are three ways to set up a H.323 call: a separate H.245 channel, fast connect and tunneling. However, it is not always possible to use fast connect or tunneling and a terminal can at any time switch back to a separate H.245 channel.

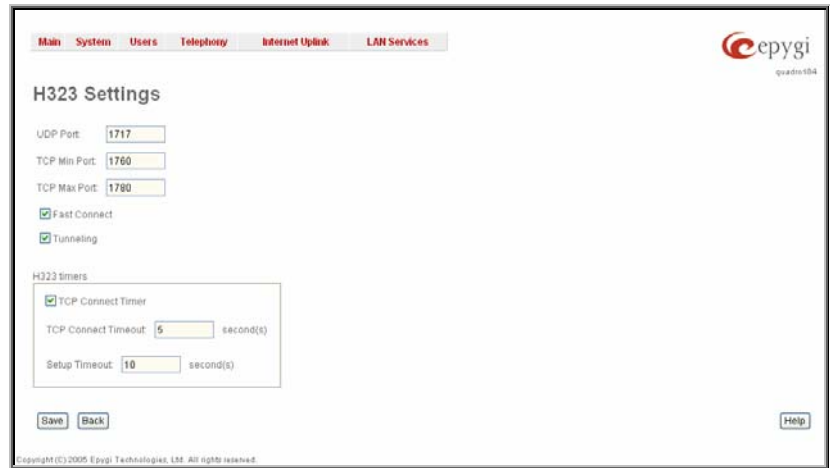


Fig. II-73: H323 Settings page

Fast Connect checkbox enables media negotiation handled by the H.225 call signaling messaging without opening H.245 channel. **Fast Connect** reduces the number of transmitted H.323 messages and allows the media channels to be operational before the connect request is sent and the telephone rings.

Tunneling checkbox enables H.245 channel to be sent within the H.225 call signaling channel.

H323 timers parameters group allows to specify TCP and Setup timeouts and provides following components:

TCP Connect Timer checkbox selection enables custom values of TCP Connect Timer (in seconds). When this checkbox is enabled, **TCP Connect Timeout** text field requires the time of TCP connection establishment. Connection establishment attempts are stopped if no connection has been established within the specified timeout.

Setup Timeout text field requires a timeout (in seconds) used on sending first signaling message if there is no any answer from the remote side.

RTP Settings

The **RTP Settings** page allows the administrator to configure the codec's packet size and silence suppression for each voice codec, to select the G726 codec standard, to define RTP/RTCP port ranges, etc. All parameters listed on this page may be modified and submitted.

The **Codec Properties** table lists all codecs with the corresponding packetization interval and information about silence suppression.

Edit opens the **Edit RTP Settings** page where the codec settings can be modified. To use **Edit**, only one codec may be selected at a time, otherwise the "One record should be selected" error message appears.

The **Packetization Interval** is the time interval between two RTP packets of the same stream. If the interval is increased, the overhead is decreased but the voice quality may deteriorate as a result. If the interval is decreased, the network load is increased and the delay is reduced.

Silence Suppression disables RTP packet transmission in case of no voice activity. This feature helps to avoid extra traffic if the RTP stream contains no voice activity. It is activated after two seconds of silence and restarted immediately if any audio appears.

The **G.726 Standard** radio buttons are used to select between packaging the G.726 codewords into octets. If you experience problems with the G.726 voice quality when one of these packaging is selected, try a different one.

- If **Use ITU-T specification** is selected, the ITU I.366.2 ("AAL2 type 2 service specific convergence sublayer for narrow-band services") type packaging of codewords is used, where packing code words into octets is starting from the most significant rather than the least significant digit in the octet.
- If **Use IETF RFC** is selected, the IETF RFC ("RTP Profile for Audio and Video Conferences with Minimal Control") type packaging of codewords is used, where packing code words is starting from the least significant position in the octet.

RTP/RTCP Port Range:

- **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.
- **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

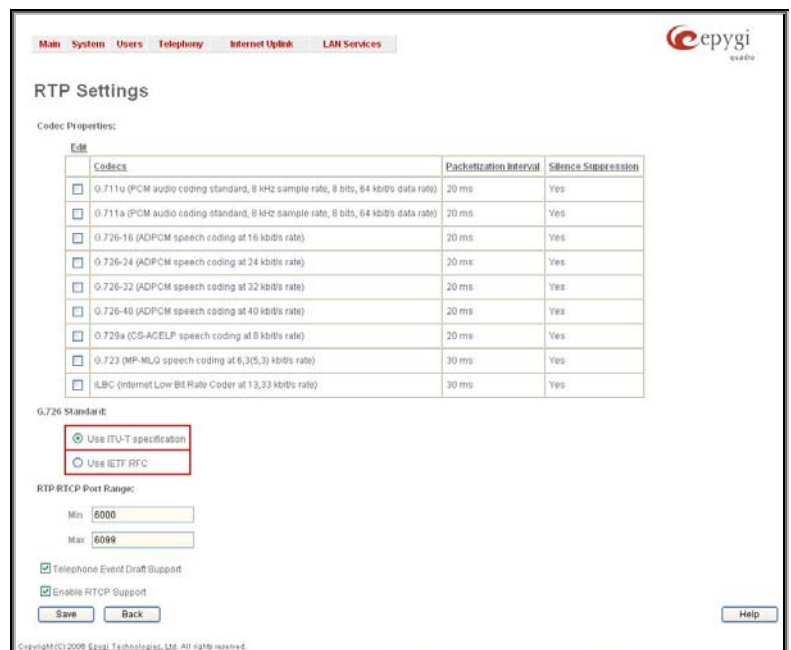


Fig. II-74: RTP Settings page

Since the specified maximum port has to be higher than the minimum port, the error message "Min port number should be less than max port number" will appear if this condition is not met. The port range must consist of digits only, otherwise the error "Incorrect Port Range: only Integer values allowed" will appear. The difference between Max and Min RTP ports should be 50 ports or less (according to the system's capabilities) otherwise the corresponding warning appears. RTP/RTCP Port ranges cannot include the defined SIP UDP ports (see [SIP Settings](#)) otherwise an error message will appear.

Telephone Event Draft Support enables telephony events transmission according to the draft-ietf-avt-rfc2833bis-04. The checkbox needs to be toggled if the SIP destination party phone or IVR has problems recognizing DTMFs generated by the Quadro.

Enable RTCP Support enables Real Time Control Protocol support and allows for the RTCP packets transmission. RTCP protocol is used for monitoring the RTP streams and changing RTP characteristics depending on Network conditions.

The **RTP Settings – Edit Entry** page offers a drop down list and a checkbox.

Packetization Interval contains possible values (in milliseconds) to be configured for the selected codec.

The **Enable Silence Suppression** checkbox selection enables voice activity detection for the selected codec.

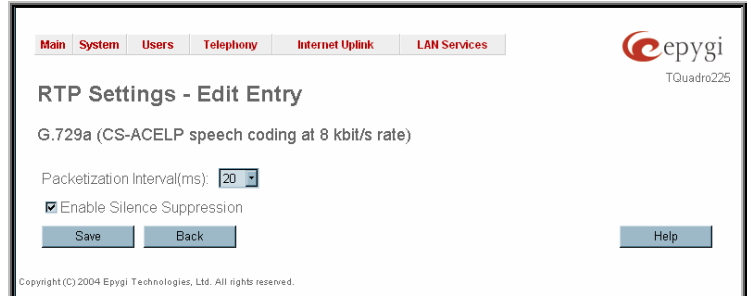


Fig. II-75: RTP Settings - Edit Entry

To Edit Codec Parameters

1. Select the codec from the **Codecs Table** that is to be edited.
2. Press the **Edit** button on the **RTP Settings** page. The **Edit Entry** page will appear in the browser window.
3. Change values in **Packetization Interval** and/or enable/disable **Silence Suppression**.
4. To save the codec settings press **Save**, or to keep the initial data click **Back**.

NAT Traversal Settings

The **NAT Traversal Settings** page is divided into separate pages used to configure SIP and H.323 NAT parameters, RTP and STUN parameters for NAT and a page where the NAT Exclusion table may be filled.

Use NAT Traversal for SIP checkbox applies to all pages and is used to enable NAT traversal for the SIP traffic, hence any incoming and outgoing SIP messages from and to the Quadro will be routed through the NAT PC.

Use NAT Traversal for H323 checkbox applies to all pages and is used to enable NAT traversal for the H.323 traffic, hence any incoming and outgoing SIP messages from and to the Quadro will be routed through the NAT PC.

The **General Settings** page consists of a manipulation radio button groups to select the mode of the NAT Traversal usage for the SIP and H.323 traffic (any incoming and outgoing SIP and H.323 messages from and to the Quadro will be routed through the NAT PC).

- **Automatic** – with this selection, system will analyze the Quadro's WAN IP address and if it is in the IP range specified for local networks (according to RFC), the SIP and H.323 traffic correspondingly will be parsed over NAT. Otherwise, if Quadro's WAN IP address is outside the specified IP range, no SIP traffic will be routed through NAT server.
- **Force** – with this selection, all SIP and H.323 traffic correspondingly will be routed through NAT server.
- **Disable** – with this selection, no SIP and H.323 traffic correspondingly will be routed through NAT server.

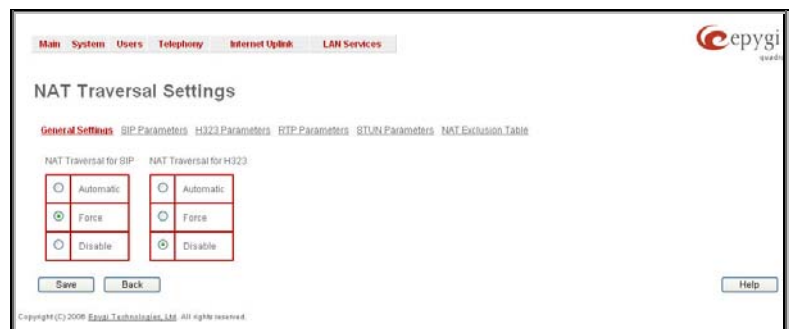


Fig. II-76: General NAT traversal page

The **SIP Parameters** page is used to configure NAT specific settings for SIP and offers two independent groups of settings:

UDP Parameters:

Manipulation radio buttons allow you to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the SIP UDP traffic over NAT. STUN settings are configured on the STUN parameters page (see below).

Selecting **Use Manual NAT Traversal** allows you to manually define the mapped settings for the SIP UDP traffic over NAT:

Mapped Host requires the IP address of the mapped host for SIP UDP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP UDP traffic over NAT.

TCP Parameters:

Mapped Host requires the IP address of the mapped host for SIP TCP traffic over NAT.

Mapped Port requires the port number on the mapped host for the SIP TCP traffic over NAT.

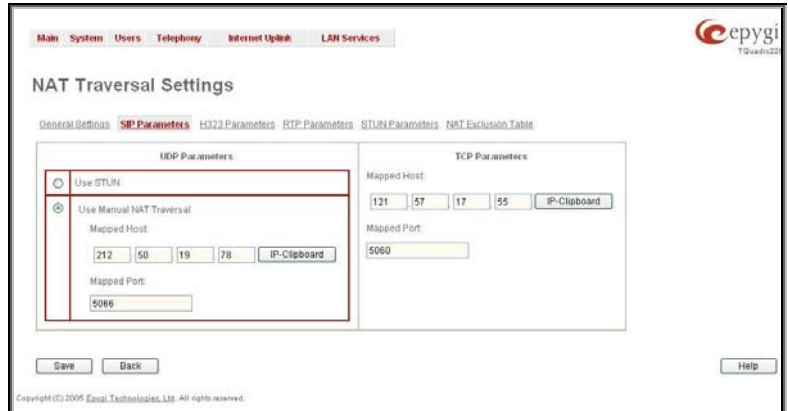


Fig. II-77: SIP Parameters page

The **H323 Parameters** page is used to configure NAT specific settings for H.323. and offers two independent groups of settings:

UDP Parameters:

Manipulation radio buttons allow you to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the H.323 UDP traffic over NAT. STUN settings are configured on the STUN parameters page (see below).

Selecting **Use Manual NAT Traversal** allows you to manually define the mapped settings for the H.323 UDP traffic over NAT:

Mapped Host requires the IP address of the mapped host for H.323 UDP traffic over NAT.

Mapped Port requires the port number on the mapped host for the H.323 UDP traffic over NAT.

TCP Parameters:

Mapped Host requires the IP address of the mapped host for H.323 TCP traffic over NAT.

Mapped Port requires the port number on the mapped host for the H.323 TCP traffic over NAT.

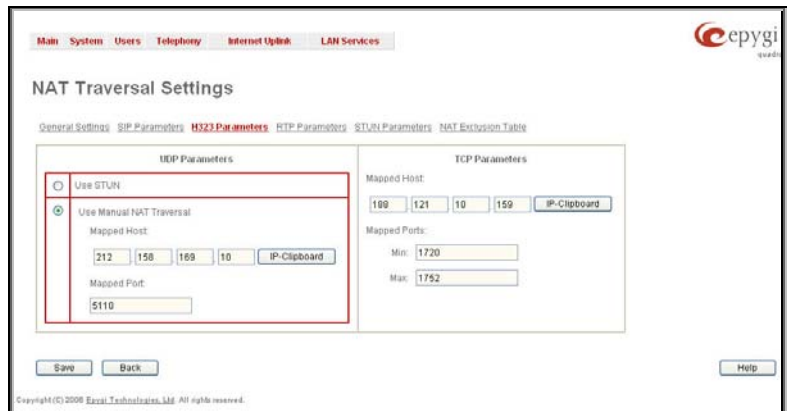


Fig. II-78: H323 Parameters page

The **RTP Parameters** page is used to choose between the STUN and Manual NAT traversal connection for the RTP traffic and to define the RTP/RTCP ports for the connection over NAT.

Manipulation radio buttons allow you to select the type of connection over NAT:

Selecting **Use STUN** will switch to automatic discovery of Mapped settings for the RTP UDP traffic over NAT. STUN settings are configured on the STUN Parameters page (see below).

Selecting **Use Manual NAT Traversal** allows you to manually define the RTP/RTCP port ranges for the RTP traffic over NAT:

- The **Mapped Host** text fields require the Mapped Host for RTP traffic over NAT.
- **Mapped RTP/RTCP Port Range:**
 - **Min** - minimal port has to be higher than 1024 and lower than the maximal port range. Only even numbers are allowed.
 - **Max** - maximal port has to be lower than 65536 and higher than the minimal port range. Only odd numbers are allowed.

Please Note: RTP/RTCP Mapped Port ranges should be greater than or equal to the RTP/RTCP port ranges defined on the [RTP Settings](#) page.

The **STUN Parameters** page enables automatic NAT configuration through the STUN server and is used to configure the STUN (Simple Traversal of UDP over NAT) client on the Quadro. This page requires the following data to be inserted:

The **STUN Server** text field requires the STUN server's hostname or IP address. The **STUN Port** text field requires the STUN server port number.

The **Secondary STUN Server** and **Secondary STUN Port** text fields respectively require the parameters of the secondary STUN server.

The **Polling Interval** drop down list contains the possible time intervals between referrals to the STUN server.

The **Keep-alive interval** text field provides the options to select the time interval (in seconds) for keeping NAT mapping alive.

The **NAT IP checking interval** text field indicates the interval (in seconds) between the NAT IP checking attempts (used to distinguish the possible NAT IP address changes and to perform registration on the new host). The value should be in the range of 10 to 3600.

The **NAT Exclusion Table** page includes a table where all possible IP ranges are listed that allows you to exclude some network addresses from being NATed. For example, if a Quadro user needs to make SIP calls within the local network as well as outside of that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table. Otherwise, a malfunction may occur in SIP operations.

The **NAT Exclusion Table** page offers the following input options:

Each record in the table has a corresponding checkbox assigned to its row. The checkbox is used to delete or to edit the corresponding record. Only one record may be edited at a time. An error message will appear if no selection is made or more than one is selected.

Each column heading in the table is a link. By clicking on the column heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

The **Add Entry** page includes the following text fields:

Add opens the **Add Entry** page where a new IP range can be added.

Edit opens the **Edit Entry** page where the IP range can be modified. This page includes the same components as the **Add Entry** page.

The **NAT Exclusion Table** lists all possible IP ranges that are not included in the NAT process, but may be accessed directly. IP addresses that are not listed in the **NAT Exclusion Table** are accessed over NAT.

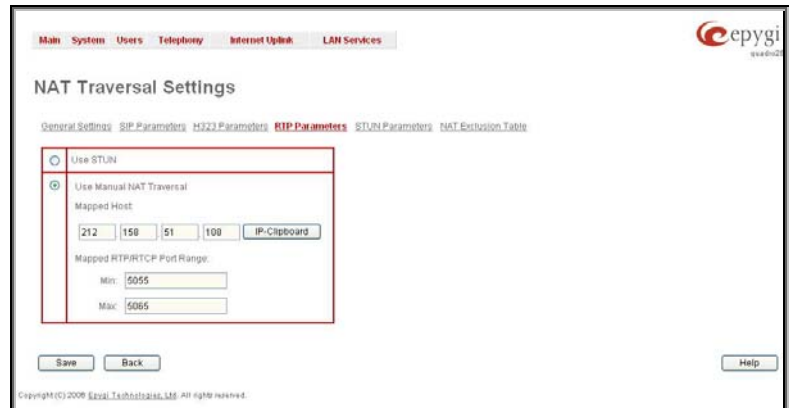


Fig. II-79: RTP Parameters page

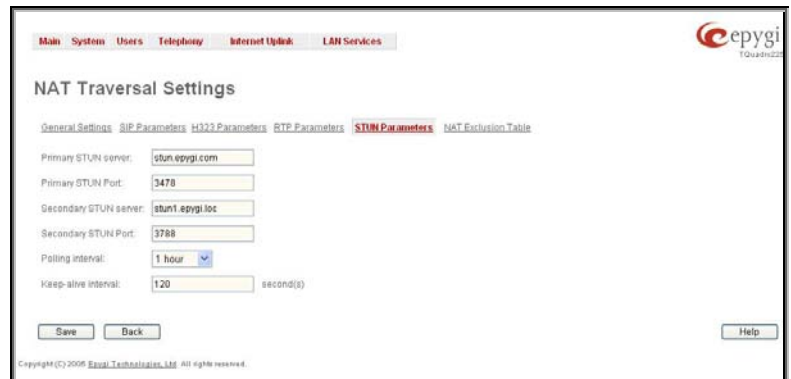


Fig. II-80: STUN Parameters page

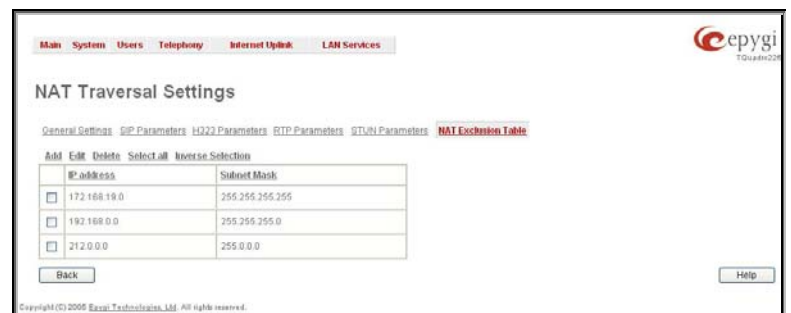


Fig. II-81: NAT Exclusion Table page

IP address requires the IP address that is placed behind NAT within the local network.

Subnet Mask requires the subnet mask corresponding to the specified IP address.

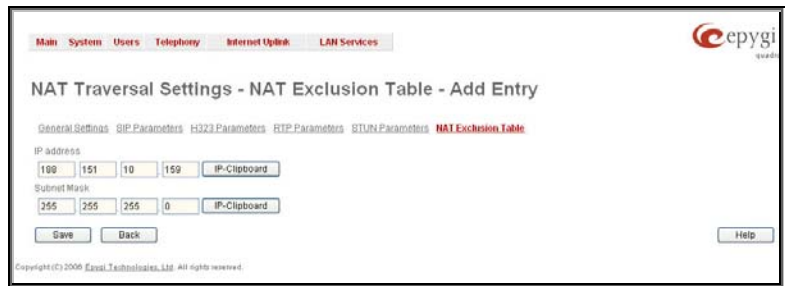


Fig. II-82: NAT Exclusion Table - Add Entry page

To Configure the NAT Exclusion Table

1. Press the **Add** button on the **NAT Exclusion Table** page. The **Add Entry** page will appear in the browser window.
2. Specify an **IP Address** and its **Subnet Mask** in the corresponding text fields.
3. Press **Save** on the **Add Entry** page to add the selected IP range to the **NAT Exclusion Table** list.

To Delete an IP Range from the NAT Exclusion Table

1. Select the checkboxes of the corresponding IP range(s) that should be deleted from the **NAT Exclusion Table**. Press **Select all** if all IP ranges should be deleted.
2. Press the **Delete** button on the **NAT Exclusion Table** page.
3. Confirm the deletion by pressing **Yes**. The IP range will then be deleted. To abort the deletion and keep the IP range in the list, press **No**.

Line Settings

The **Line Settings** are used to configure Quadro FXS Line settings.

The **Onboard Line Settings** page is used to configure Quadro lines and to define the caller ID detection type, configure remote party disconnect indication and select the ringer type on each of them. Additionally this page provides an option to enable Loopback diagnostics on the lines.

The **Onboard Line Settings** page shows the table **Available Lines** where all active lines of Quadro are listed with their **Attached Extension**. If the line is attached to an extension, the corresponding extension number is displayed in this column; otherwise "none" is displayed if the extension is not attached to the line. By clicking on the extension number, the **Extensions Management – General Settings** page will appear, where the line attached to the extension can be reconfigured. Additionally, the table provides information about the selected **Ringer Type** and **Caller ID** detection method that is configured for the selected line. The caller ID detection method is different for various types of phones and can be found in the phone manual.

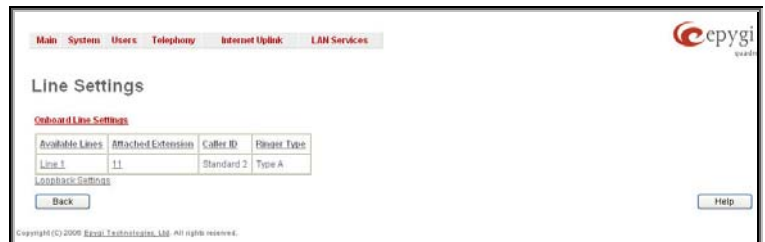


Fig. II-83: Line Settings Page

The **Loopback Settings** link takes you to the page where lines can be configured for loopback diagnostics purposes.

When pressing on the line number under the **Available Lines** column, the **Onboard Line Settings** page specific for the current line is opened and offers the following input options:

The **Caller ID** drop down list contains various standards of Caller ID transmissions. It is used to send the calling party's information to the phone attached to the selected line:

- No Caller ID.
- FSK, send prior to the first ring.
- FSK, send between the first and second ring.
- FSK, send both prior to a ring and between the first and second ring.
- DTMF, send prior to the first ring.
- DTMF, send between the first and the second ring.
- Combined, send both DTMF prior to the first ring and FSK between the first and the second rings.

The Quadro sends the current time/date to the called phone together with the caller's information.

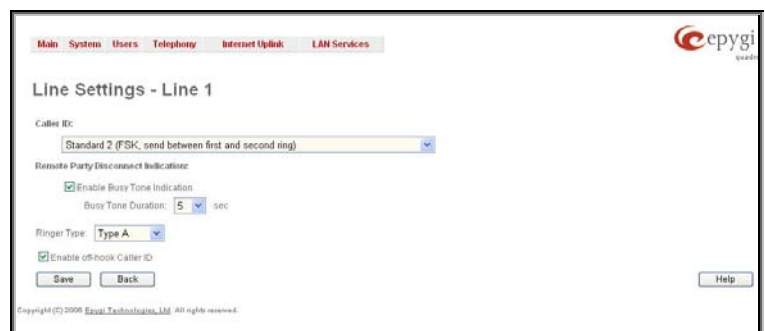


Fig. II-84: Line Codec and Caller ID Settings page

A group of **Remote Party Disconnect Indication** parameters are used to configure the private PBX attached to the Quadro FXS port.

- The **Enable Busy Tone Indication** checkbox enables a busy tone transmission to the FXS port when the remote party being called is disconnected. The **Busy Tone Duration** drop down list is used to select the period (in seconds) when a busy tone will be transmitted to the FXS port.
- The **Enable Power Disconnect Indication** checkbox enables the power cycling on the FXS line when the remote party being called is disconnected. Power Disconnect is applied after the busy tone transmission on the FXS line. The **Disconnect Duration** drop down list is used to select the period (in milliseconds) when the FXS line power will be down.

The **Ringer Type** drop down list allows you to select the frequency of the ringer supported by the phone attached to the line. Information can be found on the phone enclosure or in the phone's manual. Problems with the ringer might occur if the ringer type selected here does not correspond to the one supported by the phone.

Please Note: The supported ringer type can be found on the bottom of the phone, in the "**Ren:x.xN**" value where **N** is the ringer type supported by the phone. For example, if N=A, the TypeA ringer type should be selected, if N=B, the TypeB&Z ringer type should be selected.

The **Enable off-hook Caller ID** checkbox enables Caller ID transmission to the phone in the off-hook state attached to a certain line. Service is applicable to the phones supporting the Call Waiting Caller ID feature.

Information on the Caller ID system:

Caller ID is a service identifying the caller (when performing a call or sending a voice mail) and notifying the called party about the identity of the caller. The Caller ID service is available only for phones with a display to show that information. Two types of Caller ID notification are available on Quadro: FSK and DTMF.

FSK Standard

The FSK standard supports caller ID indication either with the phone handset on-hook or if the called party is already busy with another call or operation (handset is off-hook). For internal calls, caller ID notification in FSK can show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's extension number. The second line shows the caller's nickname (if indicated in the configuration). For external IP calls, caller ID notification in FSK can also show up to two lines of identifiable parameters on the called phone's display. The first line shows the caller's user name. The second line shows the caller's nickname (if indicated in configuration). If the nickname is not available and there is a display name, provided by the caller party, the second line will display it, otherwise the URL, in the format: username@host will be displayed. For calls from the PSTN network, the entire caller ID message will be shown.

DTMF Standard

The DTMF standard supports caller ID indication only if the phone handset is on-hook (phone is free and ready to accept calls). This standard also has caller ID notification conditions but they are non-configurable. Caller ID notification in DTMF can show only one line of identifiable parameters on the called phone's display. For internal calls, it is the caller's extension number. For external IP calls, it is the caller's user name. For calls from the PSTN network, caller ID will only display the caller's phone number.

Please Note: DTMF supports only parameters consisting of digits. If any letter symbol has been used in the external caller user name, DTMF will not display caller ID.

To Configure the Line Settings

1. Select the line number that should to be configured from the **Active Lines** column in the **Lines** table on the **Line Settings** page.
2. Press on the line number link in the **Line Settings** table. The **Line Settings - Line#** page will appear in the browser window.
3. Use the **Caller ID** drop down list to select the caller ID detection system mode corresponding to the phone type.
4. Enable the **Dialing Prefix With Caller ID** checkbox if needed.
5. Configure the **Remote Party Disconnect Indication** parameters by selecting the corresponding checkboxes.
6. Define a **Ringer Type** from the corresponding drop down list.
7. Enable **Off-hook Caller ID** if needed.
8. Press the **Save** button on the **Line Settings - Line#** page to save the caller ID system and other line specific configuration settings.

Loopback Settings

The **FXS Lines Loopback Settings** page is used to configure the lines for voice loopback diagnostics. When loopback is enabled on the line, any incoming calls to the corresponding line will automatically pick up on the first ring and any voice towards the line will automatically be sent back to the caller (the caller will hear themselves in the handset). **Loopback Timeout** provides the option of limiting the voice loopback diagnostics duration, i.e. the caller will be disconnected from the Quadro when the **Loopback Timeout** expires.

The **FXS Lines Loopback Settings** page shows the only table where all FXS lines of the Quadro are listed. On this page, the loopback diagnostics may be enabled/disabled and the Loopback Timeout can be adjusted for FXS lines.

The **FXS Lines Loopback** table lists all the FXS lines on the Quadro along with their loopback parameters (**Loopback State** and **Loopback Timeout**).

The **Edit** functional link leads to the **FXS Lines Loopback Settings - Edit Entry** page where **Loopback Timeout** (in seconds) may be configured for one or more selected FXS line(s).

The **Enable/Disable Loopback** functional link is used to enable/disable the Loopback service on the selected FXS line(s).

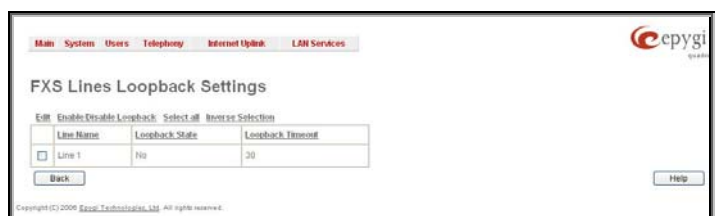


Fig. II-85: IP Line Settings –Loopback page

E1/T1 Settings

The **E1/T1 service** allows Quadro to be connected to a PBX or to a CO (Central Office) via E1/T1 lines, using E1/T1 CAS/CCS signaling. Quadro may act as a user or as network. If connected to a private PBX, the Quadro should be configured in the network mode. If an E1/T1 trunk from the CO is connected to the Quadro, it should be configured as a user.

The **E1/T1 settings** page is used to configure the E1/T1 trunk and the timeslots settings. The page consists of the following components:

The **Trunk Settings** table lists the available E1/T1 trunks on the Quadro and their settings (Trunk name, E1/T1 mode, interface, signaling types). Clicking on the trunk will open its **Signaling Settings** page (**Trunk CAS Signaling Settings** or **Trunk CCS Signaling Settings** page depending on the selected signaling type) while selecting the corresponding trunk's checkbox and pressing **Edit** will open the **Trunk – Edit Entry** page. **E1/T1 Stats** link is displayed for every active trunk on the board and refers to the page where E1/T1 trunk and traffic statistics can be viewed.

Start and **Stop** functional links are used to start/shutdown the selected E1/T1 trunk(s). When E1/T1 trunk is shutdown state, no E1/T1 calls could be placed and received.

The **Trunk – Edit Entry** page consists of the following components:

The **Interface Type** drop down list gives a option to choose between E1/T1 **User** and **Network** interface configuration.

The **Signaling Type** drop down list allows selection of **CAS** (Channel Associated Signaling) or **CCS** (Common Channel Signaling) signaling types. The same timeslot is used both for voice and data transmission in case of CAS signaling. In the case of CCS signaling a single timeslot is used for signaling data transmission on the entire trunk. All other timeslots are used for voice transmission.

The **E1** and **T1** radio buttons are used to select between E1 and T1 modes. The T1 mode enables 24 timeslots, and the E1 mode enables 32 timeslots to be used. The selection of E1 or T1 enables the **Line Code**, **Frame mode**, **Line Build Out**, **Coding Type**, **LoopBackMode** and **Clock Mode** settings. These settings are configured to match the E1/T1 settings from the service provider.

Attention: See the **Call Routing** chapter to ensure that modifications to the E1/T1 trunk settings do not lead to broken routes in the Local Call Routing Table.



Fig. II-86: E1/T1 Settings page

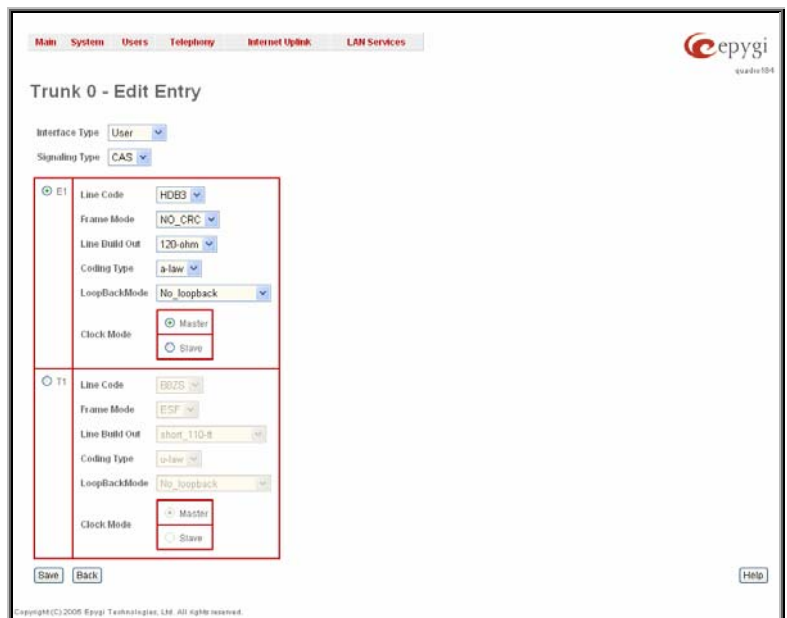


Fig. II-87: E1/T1 Settings –Edit Entry page

The **Trunk CAS Signaling Settings** page lists the available timeslots of the trunk with CAS signaling and their settings.

The [Incoming Interdigit Service](#) link leads to the page where the dial plan for incoming E1/T1 calls from CO/PBX to the Quadro can be configured.

Incoming Digits Timeout text field requires a value between 0 and 20000 (in milliseconds) and is used to define the timeout during which incoming digits from the destination party calling Quadro will be collected before being applied as an incoming called number.

Signaling Standard drop down list is available only in E1 mode and is used to select the connection signaling standard.

Force Update functional button is used to apply immediately the new settings on the selected timeslot(s). This will force the timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.

Enable/Disable functional buttons are used to enable/disable the selected timeslot(s).

Select one or more timeslots and click on **Edit** to open the **CAS Signaling Wizard** that guides through the key configuration parameters specific to the timeslot.

The **CAS Signaling Wizard** offers a possibility to configure the selected timeslot(s) and provides a variable group of parameters depending on the E1/T1 trunk configuration.

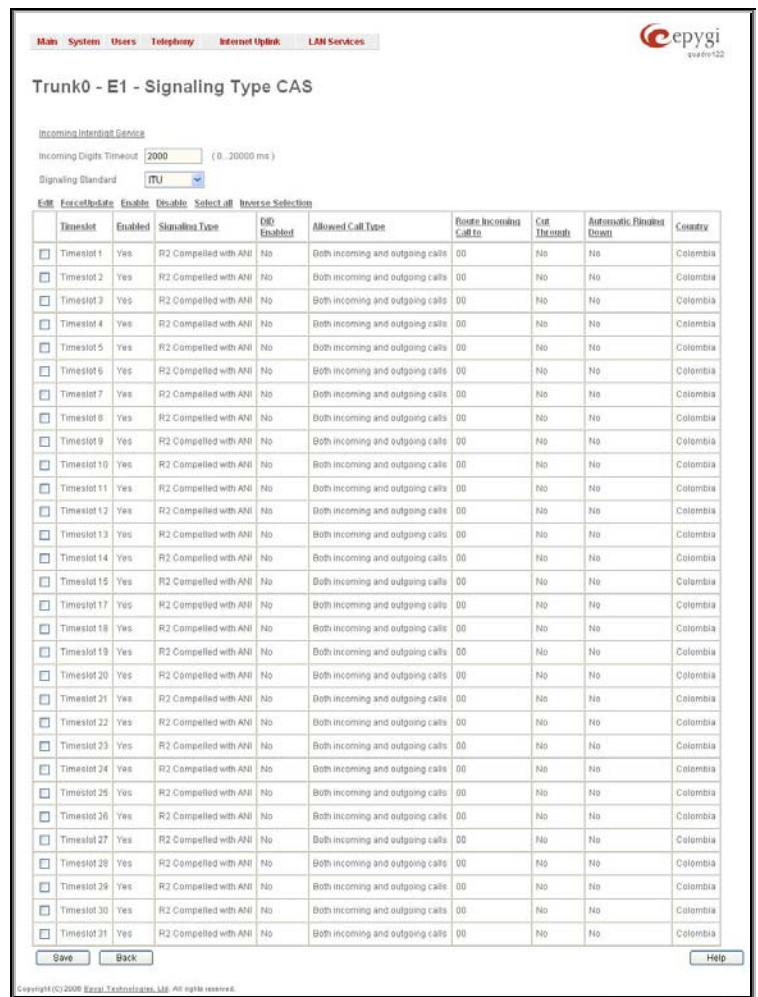


Fig. II-88: Trunk CAS Signaling Settings page

CAS Signaling Wizard – Page 1 provides a possibility to enable the **DID (Direct Inward Dialing) Service** on the timeslot(s).



Fig. II-89: CAS Signaling Wizard – Page 1

CAS Signaling Wizard – Page 2 allows to configure signaling type settings and consists of following components:

Allowed Call Type is used to select the allowed call directions: incoming, outgoing or both.

Signaling Type allows selecting the CAS signaling type.

Please Note: R2 signaling (compelled and non-compelled) can only be used with an E1 interface in User mode. Independent on the selection in this drop down list, Quadro with the T1 interface in the CAS mode is unable to detect the busy tone on the destination side. For E1 interface in the CAS mode, busy tone will be detected only for R2 compelled and non-compelled (both with and without ANI) signaling types.

Force Update Timeslots checkbox can be optionally selected in order to apply new settings immediately. This will force the timeslot(s) to be restarted and any active connection on the selected timeslot(s) will be interrupted.

Please Note: Quadro does not support the **Forward Digit** selected on the CO when acting in the **User** mode with **CAS Loop Start** signaling type.

Get PSTN/PBX Error Message checkbox enables notification message in case of outgoing calls to unreachable, incorrect or non-existent destination.

When **Generate Progress Tone to PSTN/PBX** checkbox is selected, Quadro generates ring tones to incoming callers during E1/T1 call dialing. This feature is mainly applicable to 2-stage dialing mode.

Enable Echo Cancellation checkbox enables the echo cancellation mechanism on the selected timeslot(s).

When **Alternative Disconnection Mode** checkbox is selected, the Quadro will play a busy tone towards the PBX/CO if the call has been failed. After 60 second timeout, the Quadro will disconnect the call from PBX/CO and will stop playing the busy tone.

Voice Establishment Procedure manipulation radio buttons group is used to select a method of voice establishment on the trunk:

- **On call acceptance** – with this selection, voice will be established after call is being accepted.
- **On channel selection** - with this selection, call will be accepted during channel selection. This selection is not allowed for R2 signaling.
- **On call ringing** - with this selection, voice will be established after call is being ringing. Selection enables **Generate Progress Tone** checkbox which is used to enable the progress tone generation upon voice establishment.

CAS Signaling Wizard – Page 3 allows to set the destination for incoming calls to be routed to and to enable **Cut Through** and **Automat Ringing Down** services for signaling different from R2 (all types).

Route Incoming Call to drop down appears when **Both incoming and outgoing calls** or **Incoming calls only** is selected from the **Allowed Call Type** list and allows selecting the destination where incoming calls should be routed. The list contains all extensions of the Quadro, Attendant and Routing agent. The routing agent gives two kinds of call routing possibilities in user mode and one in network mode. Choosing the **Routing** selection (available in User mode only) will request the caller to pass the authentication (if enabled) and will invite the caller to dial the destination number to connect the user within the Quadro Network. Choosing the **Routing with inbound destination number** selection will automatically use the initially dialed number to connect the destination without any additional dialing.

When **DID service** is enabled (in User mode only), incoming calls can be only routed to the Routing agent with simple **Routing** and **Routing with inbound destination number** call routing possibilities.

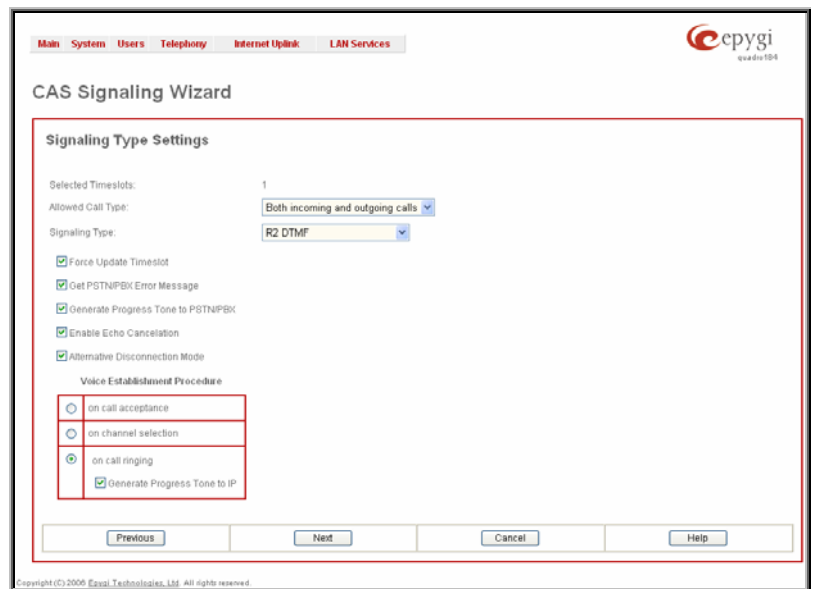


Fig. II-90: CAS Signaling Wizard – Page 2

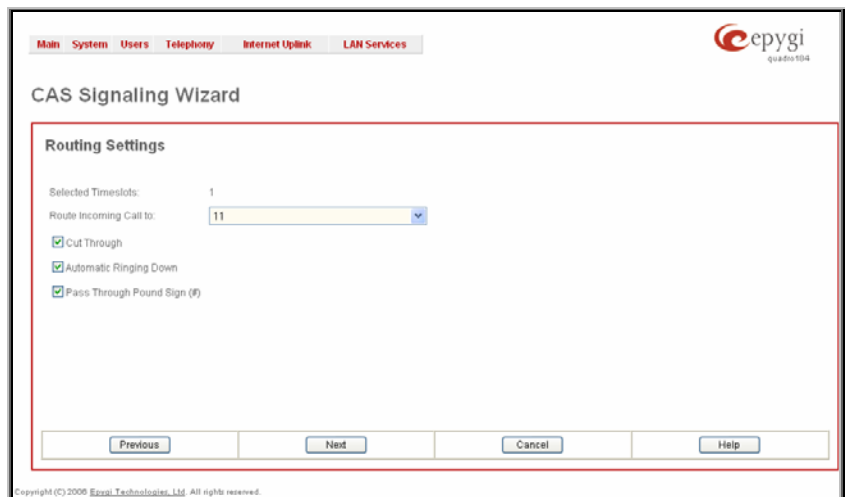


Fig. II-91: CAS Signaling Wizard – Page 3

Attention: When Quadro acts in the Network mode with the Attendant as a destination to route the incoming calls, digit forwarding should be disabled on the PBX side. Otherwise, incoming digits may be mistaken as special calling codes on the Quadro's Attendant.

Cut Through checkbox is available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from R2 (all types) and is used to reconnect the call (terminated by some reason, e.g. user error, network problems, etc.) by going on-hook and off-hook again even if the call partner is off-hook and not involved in the call.

Automat Ringing Down checkbox is available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from R2 (all types) and allows an E1/T1 device connected to the Quadro to establish a hot-line call (automatic call without any digits dialed).

Pass Through Pound Sign (#) checkbox is only available when signaling selected from the **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is different from E&M FGD or R2 (except for R2-DTMF). When this checkbox is selected, the pound sign (#) detected in the dialed number will be passed through and will be considered as a part of the dialed number. When this checkbox is not selected, the detected pound sign (#) will be considered as a call acceleration digit.

CAS Signaling Wizard – Page 4 appears only in E1 User mode when signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is R2 (all types) and is used to configure country settings. Page consists of the following components:

Country drop down list is used to set the location where Quadro is located to support the correct functionality of R2 signaling. For countries absent in this list, use **ITU** selection.

Use Default Country Settings checkbox restores default advanced settings for the selected country. When this checkbox is not selected, next page will provide a possibility to manually configure advanced country settings.

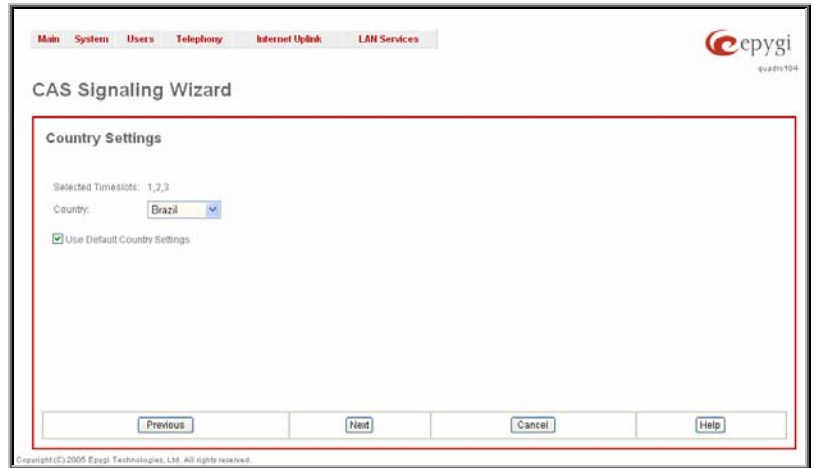


Fig. II-92: CAS Signaling Wizard – Page 4

CAS Signaling Wizard – Page 5 appears only in E1 User mode when signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard – Page 2** is R2 (all types) and when **Use Default Country Settings** checkbox is not selected on the previous page. This page is used to configure advanced country settings. Page consists of the following components:

ANI Category drop down list appears only when R2 signaling selected from **Signaling Type** drop down list on the **CAS Signaling Wizard - Page 2** is different from **R2 DTMF** is used to select the calling party priority depending on the call originator's location specifics.

ANI Request Transmit and **ANI Request Receive** drop down lists allow you to select the Caller ID request R2 tones for transmit and receive.

Seize Acknowledge Timeout text field is used to define a timeout (in a range from 2 to 2000 milliseconds) between incoming seize signal and the corresponding feedback.

Answer Guard Timeout text field is used to define a wait timeout (in a range from 0 to 1000 milliseconds) Group-B Answer Signal and Line Answer.

Release Guard Timeout text field is used to define an idle timeout (in a range from 0 to 10000 milliseconds) between the disconnect signal receipt and call disconnection.

Dialing Delay Timeout text field is used to define a timeout (in a range from 0 to 2000 milliseconds) before injecting dialed digits. Timeout specially refers to R2 DTMF signaling.

Incoming DNIS Size text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When field has 0 value, system uses either timeout defined in the **Incoming digits timeout** field or the **End of Address** messages to establish a call. Independent on the value in this field, the message **End of Address** always cause the call establishment.

Unused A:B:C:D text fields require to configure unused C and D bits of E1/T1 CAS signaling (A and B bits are predefined). Fields may have either 0 or 1 values.

Invert A:B:C:D text fields are used to invert the ABCD status bits in time-slot 16 before TX and after RX. If bit is set to 1, the router inverts it before transmission and after the receipt.

End of DNIS (I-15) checkbox is used to enable End of DNIS service.

Collect Call checkbox is only available when **Brazil** is selected in the **Country** drop down list on the previous page of the wizard and when the PBX attached to the Quadro supports this feature. When this checkbox is selected and in case of incoming calls, always the called destination will pay for the call. Option is particularly applicable when calling from the mobile phone. Checkbox should be selected when the appropriate feature is enabled on the PBX.

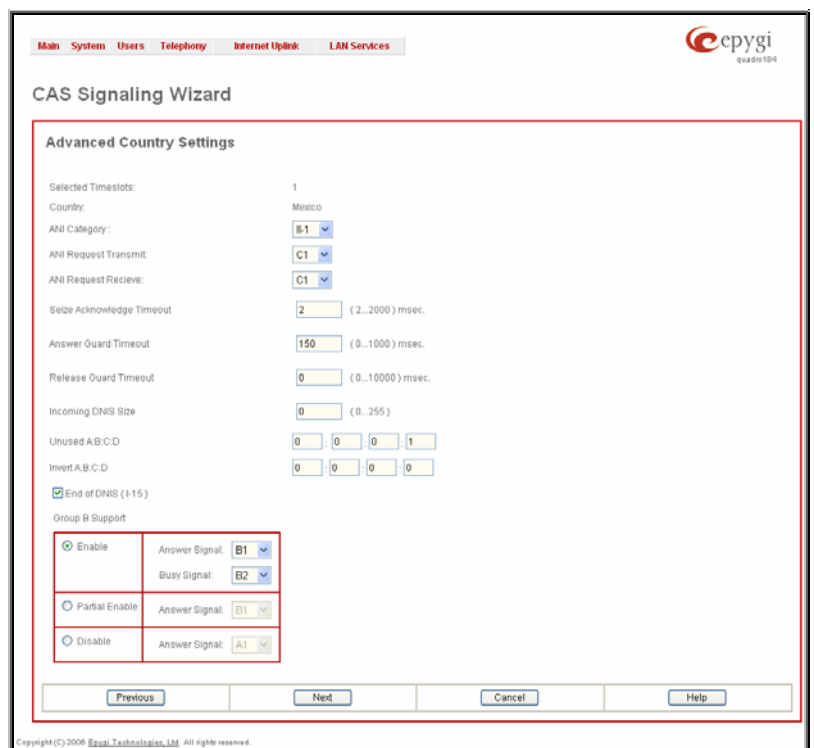


Fig. II-93: CAS Signaling Wizard – Page 5

Group B Support manipulation radio button group is present only when **R2** signaling selected from **Signaling Type** drop down list on the previous page is different from **R2 DTMF** and is used to enable/disable the **Group B Support**. The **Group B Support** manipulation radio button group offers following selection:

- **Enable** – selection enables **Group B Support** (both answer and busy recognitions are performed) and requires defining **Answer Signal** and **Busy Signal** parameters.
- **Partial Enable** – selection partially enables **Group B Support** (only answer recognition is performed) and requires defining the **Answer Signal** parameter.
- **Disable** – selection disables **Group B Support** and requires defining the **Answer Signal** parameter.

The **Trunk CCS Signaling Settings** page allows configuring CCS signaling settings and gives a possibility to select timeslots for signaling data transfer/receive and voice transfer. The page consists of the following components:

The **Non Automat** checkbox switches to non-automatic Terminal Endpoint Identifier (TEI) searching and enables the **TEI Address** text field that requires a TEI number (digit values from 0 to 63) for connection establishment between CO and E1/T1 client. In automatic mode, an E1/T1 connection will be established on the first available TEI, while in non-automatic mode a specific TEI may be reserved for the connection. In this case both call partners need to specify the same TEI in their settings.

When **Alternative Disconnection Mode** checkbox is not selected, Quadro will disconnect the call as soon as disconnect message has been received from the peer, otherwise, when checkbox is selected, Quadro's user may hear a busy tone when peer has been disconnected.

In the **Network Mode** (PBX connected):

- If **Non Automat** mode is selected, the same **TEI address** should be specified on both sides- Quadro and PBX.
- If **Automat** mode is selected the user on PBX side will have the opportunity to set any mode related to TEI assignment in PBX configuration. This will allow PBX connection to the Quadro without providing the TEI address from Quadro.

In the **User Mode** (CO connected) the TEI assignment is dependent on CO settings:

- Select **Non Automat** mode and insert the same **TEI address** provided by CO.
- Select any mode related to TEI assignment if automat TEI searching mode is selected on CO side.

Two groups of timers need to be provided. These settings are adjusted according to the Service Provider requirements.

Fig. II-94: Trunk CCS Signaling Settings page

ISDN L2 Timers:

- The **Excessive Ack. Delay T200** text field configures the period in milliseconds (digit values from 500 to 9999) between transmitted signaling packet and its acknowledgement received.
- The **Idle Timer T203** text field configures the period in milliseconds (digit values from 1000 to 99999) for E1/T1 client idle timeout.

ISDN L3 Timers:

- The **T302 Timer** text field requires the value for the T302 timer in milliseconds (digit values from 0 to 15000) and indicates the time frame system is waiting for digit to be dialed and when timer expires, it initiates the call. Timer is not applicable for DMS-100 switch types.
- The **T309 Timer** text field requires the value for the T309 timer in milliseconds (digit values from 0 to 90000) responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is 0, T309 timer will be disabled.
- The **T310 Timer** text field requires the value for the T310 timer in milliseconds (digit values from 1000 to 120000) responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) is not yet arrived.
- The **No Answer Disconnect Timer** text field requires the value for the No Answer Disconnect Timer (digit values from 0 to 200000) which is used in certain types of PBXs. The value 0 indicates that the timer is disabled. When time expires, Quadro will play a busy tone towards the PBX if the call has been disconnected by the peer.

The **D Channel Timeslot For Transmit/Receive** drop down list contains the timeslots to be selected for signaling data transmit/receive.

The **B Channel** link leads to the **Signaling Type CCS – B Channel Settings** page where available timeslots may be enabled/disabled for the voice transfer and echo cancellation feature may be configured.

The **Force Update** option can be optionally used to apply new settings immediately. The **Restart** option is used to bring timeslot(s) to the initial idle state on the both sides. When applying one of these options, any active traffic on the timeslot(s) will be terminated.

Channel Selection drop down list is used to select between the **Preferred** and **Exclusive** B channel selection methods. For **Preferred** channel selection, the CO answers to the call request by the first available timeslot, while for **Exclusive** channel selection CO should feedback only by the timeslot used for the call request.

Channel Selection Ordering drop down list is used to choose the B channels selection (Ascending or Descending). When **Ascending** selection is configured, B channels will be defined starting from B1 to B23/B30. For **Descending** selection, B channels will be defined from B23/30 to B1. If your CO/PBX has **Ascending** B channels selection configured, it is recommended to use **Descending** B channels selection and vice versa.



Fig. II-95: Trunk CCS Signaling Settings – B Channels page

Edit functional button opens **B channels – Edit Entry** page, which contains 3 checkboxes:

- Enable Timeslot – used to enable/disable the selected timeslot(s);
- Force Update Timeslot – used to apply new settings immediately by restarting the timeslot(s);
- Enable Echo Cancellation – used to enable/disable the echo cancellation feature on the selected timeslot(s).



Fig. II-96: Trunk CCS Signaling Settings – B Channels – Edit Entry page

Please Note: A timeslot can be used either for voice or data transfer. Timeslot selected for the D Channel receive/transmit is missing in the list of B channels.

The **Bearer Establishment Procedure** drop down list allows to select the session initiation method on the B channels. One of the following possibilities of the transmission path completion prior to receipt of a call acceptance indication can be selected:

- on channel negotiation at the destination interface;
- on progress indication with in-band information;
- on call acceptance.

The **Calling Party Type of Number** drop down list allows to select the type identifying the origin of call.

The **Called Party Type of Number** drop down list allows to select the type identifying the subaddress of the called party of the call.

The **Called Party Numbering Plan** and **Calling Party Numbering Plan** drop down lists indicates correspondingly the numbering plan of the called party's and calling party's number.

The **Route Incoming Call to** drop down list contains Attendant, routing agent with two kinds of call routing possibilities, and all extensions of Quadro and allows selecting the destination where incoming calls will be routed to. Choosing the **"Routing"** selection will request the caller to pass the authentication (if enabled) and will invite him to dial the destination number to connect the user within the Quadro Network. Choosing the **"Routing with inbound destination number"** selection will request the authentication (if enabled) and then will automatically use the initially dialed number to connect the destination without any additional dialing.

Attention: When Quadro acts in the Network mode with the Attendant as a destination to route the incoming calls to, digit forwarding should be disabled on the private PBX side otherwise incoming digits may be mistaken as a special calling codes on the Quadro's Attendant.

Switch Type is another configuration parameter that depends on the Service Provider when acting in the User mode and the private PBX capabilities when acting in the Network mode.

Incoming Called Digits Size text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When field has 0 value, system uses either timeout defined in the T302 field or the **Sending Complete Information element** messages to establish a call. Independent on the value in this field, **Sending Complete Information element** and pound sign always cause the call establishment.

The **Generate Progress tone on IP** checkbox selection will generate the progress tone to IP (H.323 or SIP).

When **Generate Progress Tone to PSTN/PBX** checkbox is selected, Quadro generates ring tones to incoming callers during E1/T1 call dialing. This feature is mainly applicable to 2-stage dialing mode.

Enable CLIR Service checkbox selection enables Calling Line Identification Restriction (CLIR) service which displays the incoming caller ID only in case if Presentation Indication is allowed on the remote side. Otherwise, if CLIR service is disabled, caller ID will be unconditionally displayed.

The **E1/T1 Trunk Status** page provides information about the selected trunk state. Following information is displayed on this page:

- **E1/T1 mode** - displays which mode is selected: E1 or T1.
- **Interface Type** - displays selected interface type: User or Network.
- **Signaling Type** - displays selected signaling type: CAS or CCS.
- **Clock Mode** - displays the selected clock mode: Master or Slave.
- **Framing mode** - displays selected framing mode.
- **Link** - displays E1/T1 link state: up or down.
- **Frame Synchronization** - displays the signal synchronization state in the trunk: Yes or No.
- **Red Alarm** - indicates that the receive frame alignment for the line has been lost and the data cannot be properly extracted. The red alarm is indicated by the loss of frame condition for the various framing formats.
- **Out of Frame** - number of Out of Frame errors.
- **Line Code Violation** - number of Line Code Violation errors.
- **Frame Synchronization** - number of Frame Synchronization errors.
- **Link Synchronization** - number of Link Synchronization errors.

The following statistics are available, if **CAS Signaling** is selected:

- **Active Calls** - currently active calls in the selected trunk.
- **Outgoing Calls** - total outgoing calls in the selected trunk.
- **Incoming Calls** - total incoming calls in the selected trunk.

Following statistics is available when **CCS Signaling** is selected:

ISDN PRI Layer statistics:

- **Received Packets** - number of received packets.
- **Received Errors** - number of received erroneous packets.
- **Transmitted Packets** - number of transmitted packets.
- **Transmitted Errors** - number of transmitted erroneous packets.

ISDN PRI Layer 2 statistics is displayed for actual TEI value and the received and transmitted packets:

- **TEI Value** – the actual TEI assigned
- **L2 State** – the state of the TEI assignment
- **Information Frame** - signaling packets for call initiation and termination.
- **Receive Ready** - controlling packets during E1/T1 link is up.
- **Receive Not Ready** - controlling packets in case of inability to accept calls by destination.
- **SABME** - packets upon connection establishment.
- **Disconnected Mode** - packets when connection is being disconnected.
- **Disconnect** - packets upon connection termination.
- **Unnumbered Acknowledgement** - packets upon accepting connection establishment/termination.
- **Framer** - packets as a report of an error condition.
- **TEI** - packets containing TEI (Terminal Endpoint Identifier) to initiate subscription of the device in the network.
- **Unnumbered Information Frame** - broadcast signaling packets received for call initiation and termination.
- **Exchange Identification** - received packets containing connection management settings.

ISDN PRI Layer 2 Errors statistics:

- **Incorrect Length** - packets with incorrect length.
- **Bad Supervisory Frame** - packets with incorrect supervisory header.
- **Bad Unnumbered Information Frame** - packets with incorrect unnumbered information frame header.
- **Bad Frame Type** - packets with bad frame type.
- **Bad Unnumbered Frame** - packets incorrect unnumbered acknowledgement frame header.
- **Bad TEI Value** - packets with bad TEI (Terminal Endpoint Identifier) value.

ISDN PRI Layer 3 statistics shows the same information as for CAS signaling.

No E1/T1 trunk statistics is displayed in this page at first, but page is getting automatically refreshed every 10 minutes. Statistics collected since that time and the last resetting of the counter will be displayed here.

Current System Time displays the actual time on the Quadro and the **Last Time Cleared** displays the exact date and time when the E1/T1 Stats has been manually cleared last time. **System Uptime** displays the period Quadro is on since last reboot.

To reset the statistics counters press the **Clear** button.

The screenshot shows the 'E1/T1 Status - Trunk 0' page. At the top, there are navigation tabs: Main, System, Users, Telephony, Internet Uplink, and LAN Services. The Epygi logo is in the top right corner. Below the title, there is a table for E1/T1 interface details:

E1/T1	Interface Type	Signaling Type	Clock Mode	Framing Mode	Line Code	Link	Frame Synch.	Red Alarm
T1	Network	CCS	Master	ESF	B8ZS	Up	Yes	No

Below this are summary statistics for Layer 1:

Out of Frame:	0	Frame Synchronization:	0
Line Code Violations:	0	Link Synchronization:	0

ISDN PRI statistics:

Received Packets:	19102	Transmitted Packets:	19499
Received Errors:	1	Transmitted Errors:	0

ISDN PRI Layer 2 statistics:

TEI Value:	1
L2 State:	MultiFrameEstablish

ISDN PRI Layer 2 Errors statistics:

Received:	Transmitted:
Information Frame: 8667	Information Frame: 10830
Receive Ready: 10433	Receive Ready: 8667
Receive Not Ready: 0	Receive Not Ready: 0
SABME: 2	SABME: 0
Disconnected Mode: 0	Disconnected Mode: 0
Disconnect: 0	Disconnect: 0
Unnumbered Acknowledgment: 0	Unnumbered Acknowledgment: 2
Framer: 0	Framer: 0
TEI Request: 0	TEI Request: 0
Unnumbered Information Frame: 0	
Exchange Identification: 0	

ISDN PRI Layer 2 Errors summary:

Incorrect Length:	0	Bad Frame Type:	0
Bad Supervisory Frame:	0	Bad Unnumbered Frame:	0
Bad Unnumbered Information Frame:	0	Bad TEI Value:	0

ISDN PRI Layer 3 statistics:

Active Calls:	16
Outgoing Calls:	0
Incoming Calls:	2168

System Uptime: Fri Aug 20 12:32:59 2004
 Current System Time: Fri Jan 3 16:45:42 2003
 Last Time Cleared: Thu Jul 22 16:08:59 2004

Buttons: Clear, Back, Help

Copyright (C) 2004 Epygi Technologies, Ltd. All rights reserved.

Fig. II-97: E1/T1 Trunk Stats page

Incoming Interdigit Service

The **Incoming Interdigit Service** is used to configure E1/T1 dial plan for the incoming calls from CO/PBX to the Quadro. This service allows you to speed up the call establishment procedure by detecting the prefix. The calls will be speed up by the timeout defined in the **Incoming Digits Timeout** text field.

When the system detects incoming dialed number starting with any of the prefixes listed in the **Incoming Interdigit Service** table, it will wait for the rest of the digits, as specified for the corresponding prefix in the **Incoming DNIS Size** text field (see below). Once all digits are received, the system will route the call to the destination.

The **Incoming Interdigit Service** page lists a table with existing E1/T1 dial plan entries and allows you to manage them.

By default, the table on the **Incoming Interdigit Service** page lists the locale specific (selected from the [System Configuration Wizard](#)) E1/T1 dial plan settings. For some countries, this table may however be empty.

Add functional button leads to the **Add Entry** page where a new E1/T1 dial plan entry can be configured.

The **Add Entry** page consists of the following fields:

The **Incoming DNIS Prefix** text field requires the prefix of the incoming dialed number. '[', ']', ',', '-', are used to define a range or a quantity of prefixes. For example, 2[5-9] means that the prefix of the dialed number may be 25, 26, 27, 28, or 29. 3[4,7,0] means that the prefix of the dialed number may be 34, 37 or 30. Only one range of prefixes can be defined in the **Incoming DNIS Prefix** text field.

The **Incoming DNIS Size** text field requires the total length of the dialed number, including the prefix digits. The number defined in this field should be greater than the longest prefix defined in the **Incoming DNIS Prefix** text field, otherwise the error message will appear.

The **Description** text field requires an optional description for an E1/T1 dial plan entry.

The **Restore Default Settings** functional button is used to restore the locale specific E1/T1 dial plan entries.

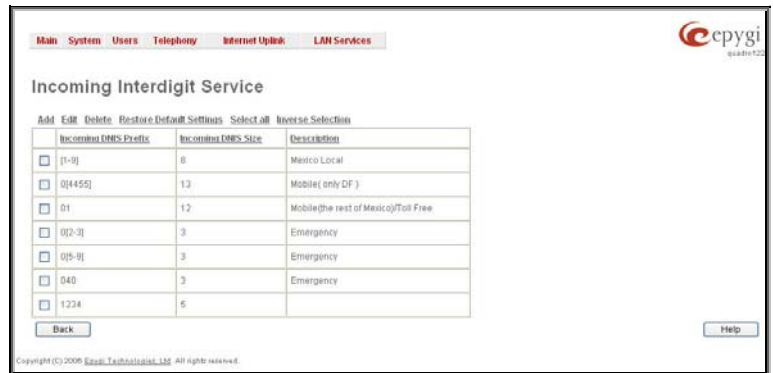


Fig. II-98: Incoming Interdigit Service page

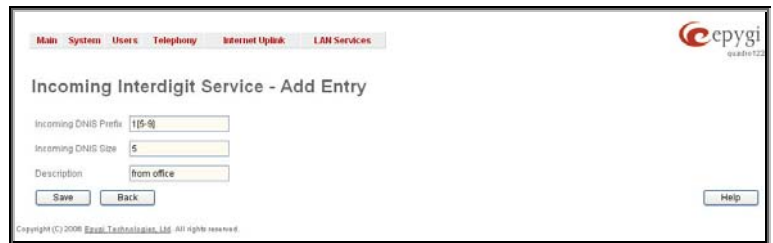


Fig. II-99: Incoming Interdigit Service – Add Entry page

Gain Control

The **Gain Control** settings are used to define transmit and receive gains. For FXS lines **Transmit Gain** defines the phone speaker volume and **Receive Gain** defines the volume of the phone microphone. For E1/T1 trunks, **Transmit Gain** defines the level of voice transmitted by Quadro to the E1/T1 network and **Receive Gain** defines the volume of voice received by Quadro from the E1/T1 network.

The **Gain Control** page consists of the **Transmit Gain** and **Receive Gain** drop down lists for each line that contain allowed gain values which can be set up by the administrator for every line.

Please Note: If gain control is configured incorrectly, DTMF digits may not be recognized properly. The gain control settings depend solely on the board location (country) and the phone type.

The **Restore Default Gains** button restores the default values.

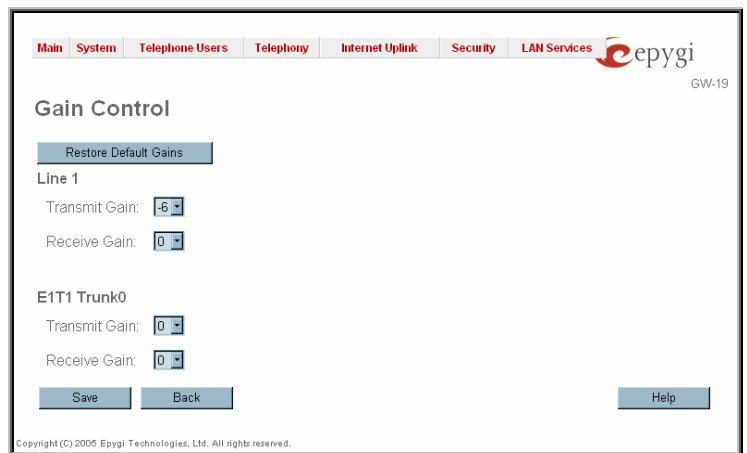


Fig. II-100: Gain Control page

Call Routing

The **Call Routing** service simplifies the calling procedure for Quadro users, i.e., different types of calls (internal, SIP, H323, PSTN or IP-PSTN) can be placed in the same way. SIP registration is not needed for extensions to make routing calls.

The **Call Routing** page offers the following components:

- The **Route all incoming SIP calls to Call Routing** checkbox that is used to route ALL incoming SIP calls (whether or not the pattern matches the extension's SIP registration username) to the Local Routing table. Digits will not be stripped in this case.
- The **Route all incoming H323 calls to Call Routing** checkbox that is used to route ALL incoming H.323 calls (whether or not the pattern matches the extension's H.323 registration username) to the Local Routing table. Digits will not be stripped in this case.
- The **Local Routing Table** link leads to the **Local Routing** table where routing patterns may be manually defined.
- The **Local AAA Table** link leads to the page where local AAA (Authentication, Authorization, and Accounting) database can be managed.



Fig. II-101: Call Routing page

ID	State	Pattern	NDS	Prefix	Call Type	IES	Destination Address	ML	URP	AAA Required	Port ID	TS	Fail Reason	Inb Caller Pattern	Inb HES	Inb Prefix	Inb Call Type	Inb Server	Inb Port ID	Inb TS	DT Period (s)	Metric	Description
1	Disabled	866	3		E1/T1					Acc	E1/T1 Trunk0	4-15,17-31	None									10	
2	Disabled	*	99	111	SIP		172.30.0.122:5060	No	No	No			None	*			E1/T1	Any				10	
3	Disabled	222	3	00	PBX					No			None									10	
4	Disabled	*			E1/T1					No	E1/T1 Trunk0		None									10	
5	Disabled	*	99	636.....1	E1/T1					No	E1/T1 Trunk0	1-15,17-31	None									10	
6	Disabled	*	99		E1/T1					No	E1/T1 Trunk0	1-15,17-31	None									10	
7	Disabled	875			E1/T1					No	E1/T1 Trunk0		None									10	
8	Disabled	5557777	3	741	SIP		sip.epygi.com:5060	No	No	No			None	102030	6	7411234	E1/T1	E1/T1 Trunk0				10	Call to sip.epygi.com
9	Disabled	1			E1/T1					No	E1/T1 Trunk0	4-15,17-31	None									10	
10	Enabled	184			E1/T1					No	E1/T1 Trunk0	1-15,17-31	None									10	
11	Disabled	*			H323 (at164)		192.168.25.155:1760	No	No	No			None	*			E1/T1	E1/T1 Trunk0	1-15,17-31			10	
12	Enabled	9*	1		E1/T1					No	E1/T1 Trunk0	1-15,17-31	None									10	
13	Enabled	777			SIP		192.168.75.204:5060	No	No	No			None									10	
14	Enabled	333	3	00	PBX					No			None	*			E1/T1	Any				10	

Fig. II-102: Call Routing table

Defining patterns in the **Local Routing Table** avoids registering Quadro at the routing management server and gives you an option to establish a direct connection to the destination or to use a SIP server or H.323 Gatekeeper for call routing.

The **Local Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and inbound caller settings, RTP Proxy and Date/Time period settings, metric and description). The value **invalid** is displayed beside the E1/T1 routing pattern, if the E1/T1 trunk settings (E1/T1 interface type, signaling type, etc.) have been changed since defining the corresponding route. Invalid E1/T1 patterns will not be allowed.

If the route has an **Authentication** or an **Authentication&Accounting** selected from the **AAA Required** checkbox group, it will have a link to the **Users List** in the **Call Routing** table. The **Users List** page contains a list of authorized users defined from the **Local AAA Table** and gives the option to enable/disable authentication of each user for a particular route.

Since the **Call Routing Table** may have multiple entries that could match to same pattern, the table will be internally rearranged according to the rules with the following consequences:

- The pattern matching best to the **Best Matching Algorithm** will have the higher position in the rearranged list
- If multiple patterns equally match to the **Best Matching Algorithm**, the pattern with the lower metric will get the higher position in the rearranged list
- If the multiple patterns with the same metric have been matched to the **Best Matching Algorithm**, the pattern in the higher position in the table will get the higher position in the rearranged list.

The pattern in the highest position of the rearranged list will be considered as the preferred one. The second and subsequent matching patterns will be used, if the destination refused the call due to the configured Fail Reason.

The **Enable/Disable** functional buttons are used to enable/disable the selected route(s). Disabled routes will have no effect. Enabled routes will be parsed when initiating routing calls. The **State** column in the **Call Routing Table** displays the current state of the routes (enabled/disabled).

Add starts the **Call Routing Wizard** where a new routing pattern may be defined. The **Call Routing Wizard** is divided into several pages. Page 1 displays the following components:

Pattern requires entering the routing pattern's identification. To make a specified call, the appropriate routing pattern should be dialed. Wildcards are allowed here (see chapter [Entering a SIP Addresses correctly](#)). '[', ']', ',', '-', '{', '}' are used to define a range or a quantity of numbers, '!' symbol is used for exclusion ("!5a" inserted in Pattern field means all patterns except those equal to 5a). For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified pattern; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified pattern.

Number of Discarded Symbols (NDS) requires the number of symbols that should be discarded from the beginning of the routing pattern. The field should be empty if digits do not need to be discarded. Only numeric values are allowed for this field, otherwise an error message "Error: Number of Discarded Symbols is incorrect - digits allowed only" appears.

Prefix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in front of the routing pattern instead of the discarded digits.

Suffix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in the end of the routing pattern. For example, if the routing **Pattern** is 12345, the **Number of Discarded Symbols** is two, and the **Prefix** is 909 and **Suffix** is 0a, the final phone number will be 9093450a.

Call Type gives you the option to select the call type (PBX, PBX-Voicemail, H323, SIP, IP-PSTN or E1/T1). The **PBX** call type is dedicated for call routing to the local PBX extension, and the **PBX-Voicemail** call type is dedicated to route the calls directly to the voice mailbox of the local PBX extension.

Metric allows entering a rating for the selected route in a range from 0 to 20. If a value is not inserted into this field, 10 will be used as the default. If two route entries match a user's dial string, the route with the lower metric will be chosen.

The **Description** text field requires an optional description of the routing pattern.

The **Filter on Caller / Call Type / Modify Caller ID** checkbox selection allows limiting the functionality of the current route to be used by the defined caller(s) only. If this checkbox is enabled, inbound caller information (**Inbound Caller Pattern**, **Inbound Call Type**, **Inbound Port ID**, etc.) will be required later in the **Call Routing Wizard**.

The **Set Date / Time Period(s)** checkbox selection allows you to define a validity period(s) for current routing patterns to take place and to define pattern date/time rules. When this checkbox is enabled, the **Call Routing Wizard** - Page 5 will be displayed.

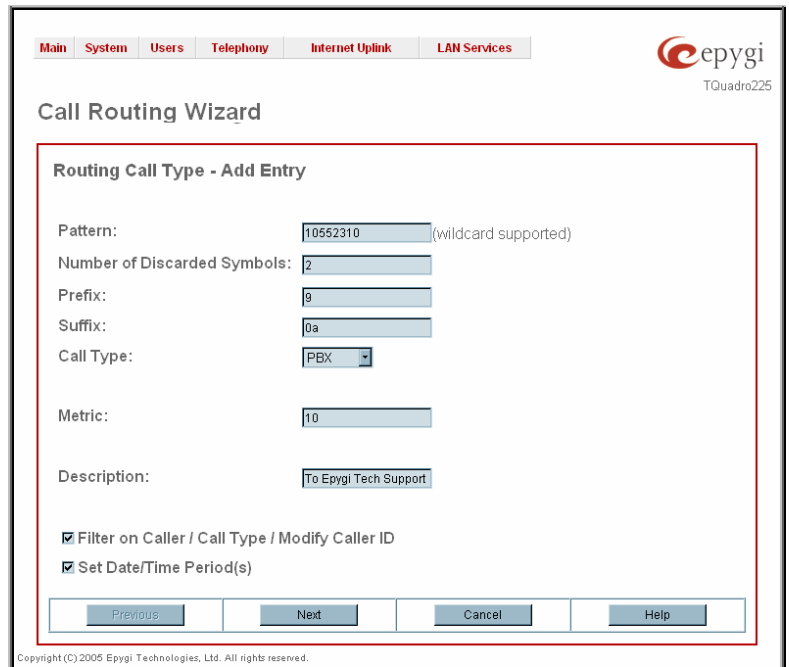


Fig. II-103: Call Routing Wizard - page 1

The second page of the **Call Routing Wizard** offers different components depending on the **Call Type** selected on the previous page.

Use Extension Settings drop down list is applicable to SIP, H.323 and IP-PSTN call types and allows you to select the extension (also Auto Attendant) on behalf of the call that will be placed. The SIP and H.323 settings of the selected extension will be used as the caller information. If an entry is not selected from this list, the original caller information will be kept. When **Keep original DID** checkbox is selected, the called destination will receive the original caller's information and not the information of the extension selected from the **Use Extension Settings** list.

Destination Host requires the IP address or the host name of the destination (for a direct call) or the server (for calls through the SIP server or H323 gatekeeper).

Destination Port requires the port number of the destination or of the SIP server or H323 gatekeeper.

H323 Alias field is actual for H323 call type only and may contain different characters: for **e164** user name type digit characters allowed only, **h323-ID** user name type allows any characters for the registration user name.

User Name and **Password** require the identification settings for the public SIP server or servers requiring authentication.

Fig. II-104: Call Routing Wizard - page 2

The **Multiple Logons (ML)** checkbox is only available for the IP-PSTN call type and allows/denies multiple logon to the public SIP server with the same username at the same time.

Enable Activity Timeout checkbox is used to limit time-to-live period of routing pattern (makes sense if accept or failure feedback arrives too late from the destination). Checkbox selection enables the **Activity Timeout** text field which is used to insert a routing pattern activity timeout (in the range from 1 to 180 seconds). When timeout is configured, the routing pattern will be active within the defined time frame and if no response has been received from the destination during that period, the pattern will be stopped and next routing rule might be optionally considered (depending on the **Fail Reason** configuration on the corresponding pattern).

The **Use RTP Proxy** checkbox is available for SIP, H.323 and IP-PSTN call types and is applicable when a route is used for calls through Quadro between peers that are both located outside the Quadro. When this checkbox is selected, RTP streams between external users will be routed through Quadro. When the checkbox is not selected, RTP packets will move directly between peers.

Voice Transcoding checkbox is available for **SIP, H323** and **IP-PSTN** call types and is meaningful when an extension is selected from the **Use Extension Settings** drop down list. Checkbox selection results the voice transcoding when performing IP calls through Quadro. Independent on the codecs supported by the caller, Quadro will use the codecs of the extension selected from the **Use Extension Settings** drop down list to establish a call with the Destination. If the Destination supports either of the codecs configured for the used extension, the call between the caller and the Destination will be established by the first preferred codec of the Destination. If the Destination does not support either of the codecs configured for the used extension, the call will be disconnected.

The **AAA Required** checkboxes are used to choose one or more of the following Authentication, Authorization, and Accounting (AAA) settings:

- **Local Authentication** – with this checkbox selected, callers will need to pass authentication through the Local AAA table (see below) when dialing the current pattern.
- **RADIUS Authentication and Authorization** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, callers will need to pass the authentication through RADIUS server (see above) when dialing the current pattern.
- **RADIUS Accounting** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, authentication will not take place, but a caller identifying a CDR (call detail report) will be sent to the RADIUS server. This checkbox selection enables accounting on the RADIUS for a certain call. This selection enables the **Client Code Identification** checkbox which is used to activate/deactivate the code identification on the RADIUS server. When the **Client Code Identification** checkbox is selected, caller may optionally dial an identity code at the end of the corresponding route. To make an identified call, caller should dial **Routing Number + * + Identity Code**. Here, **Identity Code** is an arbitrary digit combination used to identify the corresponding routing rule. Identity Code can be used to identify certain called destinations. This will allow to search the calls by the certain identity code criteria on the RADIUS server (for example, for further billing calculation purposes).

If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.

The **Fail Reason** drop down list shows the available failure reasons, depending on the call type selection on the previous page. The following Fail Reasons may be available in this list:

- **Cannot Establish Connection** - failure reason is only available for E1/T1 calls and indicates cases when a connection cannot be established.
- **Wrong Number** – available for PBX, SIP, H323 and IP-PSTN call types and indicates cases when the dialed number is wrong.
- **Busy** - available for PBX, SIP, H323 and IP-PSTN call types and indicates cases when the dialed destination is busy.
- **Network Failure** - available for SIP, H323 and IP-PSTN call types and indicates cases of system overload, network failure or timeout expiration occurred.
- **Other** - available for SIP, H323 and IP-PSTN call types and indicates cases of authorization, negotiation, not supported, request rejected or other unknown errors occur.
- **System Failure** - available for SIP, H323 and IP-PSTN call types and indicates cases of **Network Failure** and **Other** fail reasons.
- **None** – available for all call types and indicates no failure reason.
- **Any** - available for all call types and indicates any of the above mentioned failure reasons.

If the call cannot be established due to some of the selected Failure Reason, the call routing table will be parsed for the next matching pattern and, if found, the call will be routed to the specified destination.

The **SIP Privacy** manipulation radio buttons group is only available for the **SIP** call type and allows you to select the security of the SIP route by means of hiding (or replacing, depending on the configuration of the SIP server) the key headers of the SIP messages used to establish the call.

- **Default Privacy** – with this selection, Quadro specific SIP privacy will not be applied and all privacy will rely on the configuration of the SIP Server.
- **Disable Privacy** – with this selection, SIP call security will not be disabled and all headers of the SIP message will be transparently visible to the destination.
- **Enable Privacy** - with this selection, SIP privacy will be specified for the corresponding route. This selection enables a group of checkboxes in order to choose the key headers that are to be fully or partly hidden or replaced. The **Require Privacy** checkbox selection is used to restrict the delivery of the SIP message if any of the selected headers cannot be hidden (or replaced, depending on the configuration of the SIP server) before being sent to the destination.

The **Port ID** drop down list is present for E1/T1 call type and contains available E1/T1 trunk(s). In case the E1/T1 call type has been selected the available Timeslots (TS) should be selected on the next page.

The **Local Call Routing Wizard** - Page 3 appears if the **Fill Call Source Information** checkbox had been enabled on Page 1 of the **Local Routing Wizard**. It will require information about the Inbound caller.

The **Inbound Caller Pattern** field requires the caller's address where the current route will be applied. Alphanumerics and any characters supported in the SIP username/H323 gatekeeper are allowed for this field. Wildcards are allowed here (see chapter [Entering a SIP Addresses correctly](#)). '[', ']', '{', '}', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified pattern; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified pattern.

The **Inbound Number of Discarded Symbols** and **Inbound Prefix** text fields are hidden only when an **FXO** call type has been selected from Page 1 of the **Call Routing Wizard**. The **Number of Discarded Symbols (NDS)** text field requires the number of digits that should be discarded from the beginning of the **Inbound Caller Pattern**. The field should be empty if digits do not need to be discarded. Only numerics are allowed for this field, otherwise the error message "Error: Number of Discarded Symbols is incorrect - digits allowed only" will appear.

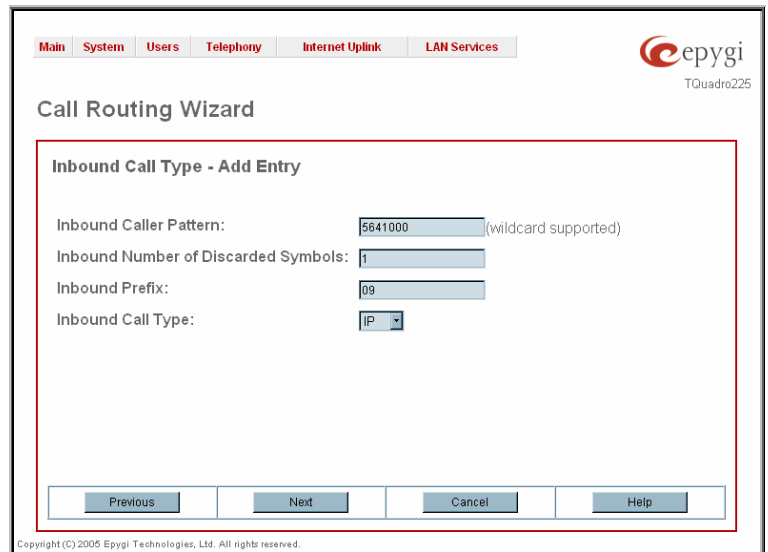


Fig. II-105: Call Routing Wizard - page 3

The **Inbound Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Inbound Caller Pattern** instead of the discarded digits. (For example, if the routing pattern is 12345, the Number of Discarded Symbols is two, and the prefix digits are 909, the final phone number will be 909345.) Wildcards are allowed here (see chapter [Entering a SIP Addresses correctly](#)).

The **Inbound Call Type** drop down list gives you the option to select the call type (PBX, SIP, H323, E1/T1) used by the inbound caller to reach the Quadro.

The **Next** button will open the **Local Call Routing Wizard** - Page 4 where different information about Inbound Caller will be required depending on the selected **Inbound Call Type**. For the **SIP** and **H323** Inbound Call Type, the **Inbound Host** text field will require one or more IP addresses or host names of the SIP server/H323 gatekeeper where the caller is registered, or the caller's device if they are direct calls, separated by a space. In case of **E1/T1** Inbound Call Types selected, **Inbound Port ID** drop down list will require to select the Trunk ID number, and in the next step, a list of timeslot(s) used to receive calls from the defined caller.

The **Call Routing Wizard** - Page 5 appears if the **Set Date / Time Period(s)** checkbox previously had been enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the pattern validity period(s).

This page provides selection between **Typical** and **Custom** date/time rule definitions.

The **Typical** selection contains the following group of radio buttons that are used to select the frequency of the corresponding routing pattern that is to take place:

- **Daily**
- **Weekly** – the preferred weekday(s) should be selected for this option.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and month should be selected for this option.

In the **Available Time Period** drop down lists, the time range of the pattern validation should be defined. Any time selected in this field will be considered corresponding to the [Time/Date Settings](#).

The **Custom** selection provides the option to manually define the validity period(s). Use the following format to insert pattern date/time rule(s):

[Month,Month-Month,...][Day-Day,Day,...][hh:mm-hh:mm,...]; ...



Fig. II-106: Call Routing Wizard - page 5

The **Duplicate** functional button is used to create a routing pattern with the settings of an exiting one. This is to avoid configuring a new routing entry completely by duplicating an existing entry with different settings. To use the **Duplicate** button only one record may be selected, otherwise the error message "One row should be selected" will appear. The **Duplicate** button opens the **Call Routing Wizard** where all fields except the **Pattern** field are already filled in. A **Pattern** for the new route will be required anyway.

The **Move Up/Move Down** buttons are used to move call routing patterns one level up or down within the **Call Routing** table. The sequence of the routing patterns is important when making routing calls because the **Call Routing** table is parsed from the top down and routing will take place according to the first pattern that matches the dialed number. The **Move To** button is used to move the selected entry to a different position in the Call Routing Table. This will increase or decrease the selected pattern's priority. Pressing the button will open the page where a row number should be specified together with the position the selected entry is to be placed (before or after the defined row).

The **Local AAA Table** page allows you to manage local authentication and the authorization database. Callers dialing the routes which have an AAA (Authentication, Authorization, and Accounting) option enabled, will pass the authorization on the **Local AAA Table** by using a phone number or username/password, depending on the corresponding entry configuration on this page.

The caller passes authorization automatically if the detected phone number of the caller dialing a route has the AAA option enabled and is registered in the **Local AAA Table**. If the caller ID service is disabled or the caller's phone number is not registered, the caller is asked to enter a registration user name and password.

The **Add** functional button opens the **Call Routing – Local AAA Table - Add Entry** page where a new local AAA record can be created.

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the type of authorization and the following other parameters:

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller's phone number (which is considered to be automatically detected). The **Phone Number** text field requires the caller's phone number. Only numeric and wildcard characters (see chapter [Entering a SIP Addresses correctly](#)) are allowed for this field. '[', ']', ',', '!', '{', '}' are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number.

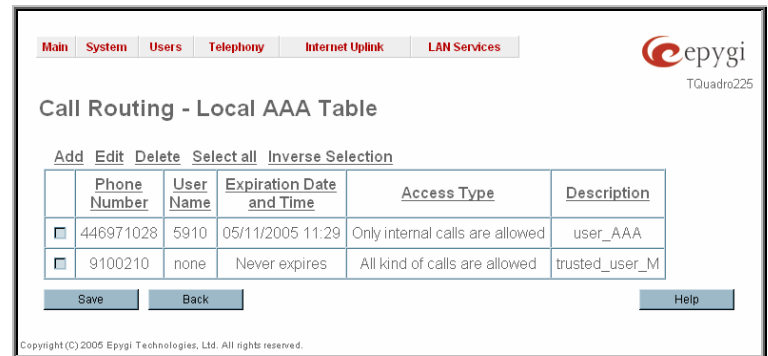


Fig. II-107: PSTN User Registration page

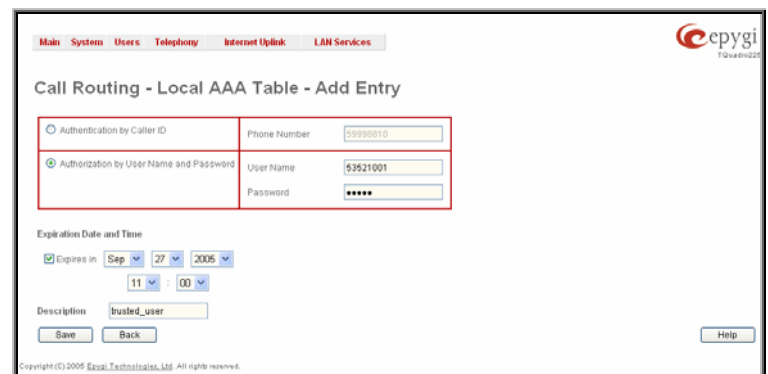


Fig. II-108: PSTN User Registration - Add Entry page

- **Authorization by Username and Password** – this selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication username. Only numeric values are allowed for this field, otherwise the error message "Incorrect Username - digits allowed only" will appear. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the error message "Incorrect Password - digits allowed only" will appear.

The **Expiration Date and Time** drop-down lists are used to set the date and time when the registration will expire.

The **Expires in** checkbox is used to enable the **Expiration Date and Time** feature.

The **Description** text field requires an optional description about the calling party.

To make a Local Routing pattern

1. Click on the **Call Routing Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Call Type** from the drop down list.
6. Define the **Metric** or leave the default.
7. Enter a **Description** if needed.
8. Enable the **Filter on Caller / Call Type / Modify Caller ID** checkbox, if the route functionality should be limited depending on inbound caller information.
9. Enable **Set Date/Time Period(s)** checkbox, if route should be functional within certain time/date interval.
10. Press **Next**.
11. Select the user or attendant extension from the **Use Extension Settings** drop down list that the call will be placed on.
12. Specify the **Destination Host** and **Port Number**, **Username** and **Password** if an **SIP**, **H323** or **IP-PSTN** call type has been selected. Additionally select the **H323 Alias** from the same named drop down list if **H323** call type has been selected. For the **IP-PSTN** call type, enable **Multiple Logons** if necessary. For **E1/T1** call type choose one or more timeslots from the **Timeslots** list. Enable the **Use RTP Proxy** checkbox if needed.
13. Choose the Authentication and Accounting method from the **AAA Required** drop down list.
14. Choose a **Fail Reason** from the corresponding drop down list.
15. Press the **Next** button.
16. If the **Filter on Caller / Call Type / Modify Caller ID** checkbox has been previously enabled and the call type is different from the E1/T1, fill in the **Inbound Caller Pattern** into the corresponding text field. Choose the needed value from the **Inbound Call Type** drop down list, as well as the **Inbound Number of Discarded Symbols** and **Inbound Prefix** values.
17. Press the **Next** button.
18. If **SIP** or **H323** has been selected on the previous step in the **Inbound Call Type** drop down list, then **Inbound Host** should be inserted in the current page. If **E1/T1** has been selected in the **Inbound Call Type** drop down list, **E1/T1 trunk** number followed by the list of timeslots should be selected here.
19. If the **Set Date/Time Period(s)** checkbox has been selected on the first page, pressing **Next** will open the **Date/Time Rules** page where route validity should be defined.
15. Press the **Finish** button to establish a local route with the inserted settings.

To create a local AAA entry

1. Click on the **Local AAA Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Local AAA Table** page.
3. Choose the Authentication type.
4. Enter the **Phone Number** or the **Username** and **Password** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

Best Matching Algorithm

The **Best Matching Algorithm** is used by the Routing Agent (RA) to sort the list of patterns that match a dialed number. Sorting is done by the following principle: **the more the pattern matches the dialed number, the higher its priority.**

To decide which of the selected patterns matches the dialed number more in comparison with the other patterns, the following list of criteria is used (List 1). The criteria are ordered by their priorities: that is Criterion 2 is calculated only if more than one pattern takes the same value for Criterion 1, Criterion 3 is calculated only if more than one pattern takes the same value for Criterion 2, etc. **Each consecutive criterion is calculated only if more than one pattern takes the same value for the preceding criteria.**

List 1

Criterion 1	The presence of asterisks (“**”) in a pattern The patterns without “**” have higher priority.
Criterion 2	The number of matching digits/symbols The more matching digits a pattern has, the higher its priority.
Criterion 3	The number of square brackets (“[]”) The more ranges a pattern has, the higher its priority.
Criterion 4	The number of question marks (“?”) The more question marks a pattern has, the higher its priority.
Criterion 5	The number of braces (“{}”) The more ranges a pattern has, the higher its priority.
Criterion 6	The number of asterisks (“**”) The fewer asterisks a pattern has, the higher its priority.
Criterion 7	The value of the metric The lower the metric of a pattern is, the higher its priority.
Criterion 8	The position in the routing table The higher the position of a pattern in the routing table is, the higher its priority.

The algorithm is discussed in the example below.

Example The user has dialed 1231 and the Routing Agent has found the following list of matching patterns.

The list of matching patterns found by RA
1
123*
{11-15}3*
?2?1
123?
[1-3]*
[1-3]???
{100-150, asd, *?}1
12*31
1[1-3]3[0-8]
1231
*2*1
*

The step-by-step discussion of the **Best Matching Algorithm** is as follows.

Step 1: The list is split into two groups separating the patterns with “**” from the ones without (Criterion 1). The patterns with “**” form a group with lower priority and are pushed back to the end of the list (Table 1).

Table 1 The list split into two subgroups
?2?1 123? [1-3]??? {100-150, asd, *?}1 1[1-3]3[0-8] 1231
1 123* {11-15}3* [1-3]* 12*31 *2*1 *

Step 2: The two groups of patterns are sorted separately from each other by the number of matching digits in descending order (Criterion 2, Table 2). The patterns that have the same number of matching digits are grouped into sub-lists (Table 3). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 2

The list of patterns	Criterion 2
1231	4
123?	3
???1	2
1[1-3]3[0-8]	2
{100-150, asd, \^?}1	1
[1-3]???	0
12*31	4
123*	3
*2*1	2
1	1
{11-15}3*	1
[1-3]*	0
*	0

Table 3

The list of patterns	Criterion 2
1231	4
123?	3
???1	2
1[1-3]3[0-8]	2
{100-150, asd, \^?}1	1
[1-3]???	0
12*31	4
123*	3
*2*1	2
1	1
{11-15}3*	1
[1-3]*	0
*	0

The principle by which the patterns have been sorted in Step 1 is applied in all further steps with a different criterion.

Step 3: Each sub-list is sorted separately from the others by the number of brackets (“[]”) in the pattern in descending order (Criterion 3, Table 4). The patterns that have the same number of ranges are grouped into sub-lists (Table 5). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 4

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	2
???1	0
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	1
*	0

Table 5

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	2
???1	0
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	1
*	0

Step 4: Each sub list is sorted separately from the others by the number of question marks in the pattern in descending order (Criterion 4, Table 6). The patterns that have the same number of question marks are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 6

The list of patterns	Criterion 3
1231	-
123?	-
1[1-3]3[0-8]	-
???1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
1	0
{11-15}3*	0
[1-3]*	-
*	-

Step 5: Each sub-list is sorted separately from the others by the number braces (“{ }”) in the pattern in descending order (Criterion 5, Table 7). The patterns that have the same number of ranges are grouped into sub-lists (Table 8). If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Table 7

The list of patterns	Criterion 4
1231	-
123?	-
1[1-3]3[0-8]	-
?2?1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
{11-15}3*	1
1	0
[1-3]*	-
*	-

Table 8

The list of patterns	Criterion 4
1231	-
123?	-
1[1-3]3[0-8]	-
?2?1	-
{100-150, asd, \^?}1	-
[1-3]???	-
12*31	-
123*	-
*2*1	-
{11-15}3*	1
1	0
[1-3]*	-
*	-

Step 6: This step is applicable to the subgroup containing patterns with "*", the group with lower priority. Each sub-list is sorted separately from the others by the number of asterisks ("*") in ascending order (Criterion 6). The patterns that have the same number of asterisks are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.

Step 7: Each sub-list is sorted separately from the others by the value of metric in ascending order (Criterion 7). The patterns that have the same value of metric are grouped into sub-lists. If a sub-list consists of one pattern, it stays in its position and does not participate in further discussions.
The values of metrics are taken from the routing table.

Step 8: The patterns in each sub-list are arranged by their positions in the routing table (Criterion 8).

The subgroup containing patterns with "*" is attached to the end of the subgroup without "*" forming a single list of sorted patterns. The obtained list is the sorted list of the patterns by the Best Matching Algorithm (Table 9).

Table 9 The sorted list of patterns
1231
123?
1[1-3]3[0-8]
?2?1
{100-150, asd, \^?}1
[1-3]???
12*31
123*
*2*1
{11-15}3*
1
[1-3]*
*

VoIP Carrier Wizard

The **VoIP Carrier Wizard** is used to define access codes for available VoIP Carrier accounts which will particularly allow you to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

For each configured VoIP carrier, the wizard creates a specific IP-PSTN routing rule in the [Call Routing](#) table. Additionally, a virtual extension automatically generated in [Extensions Management](#) will be registered on the defined VoIP Carrier's SIP server. The settings of that extension will be used to make calls from Quadro's users towards the created VoIP Carrier will be placed.

VoIP Carrier Wizard – Page 1 provides a following option of describing the VoIP carrier:

When predefined carrier is selected in the **VoIP Carrier** drop down list, the SIP Server and Port will be already predefined in the next page. **Manual** selection allows you to manually set up the VoIP Carrier settings.

The **Description** field allows you to insert an optional description of the VoIP Carrier.

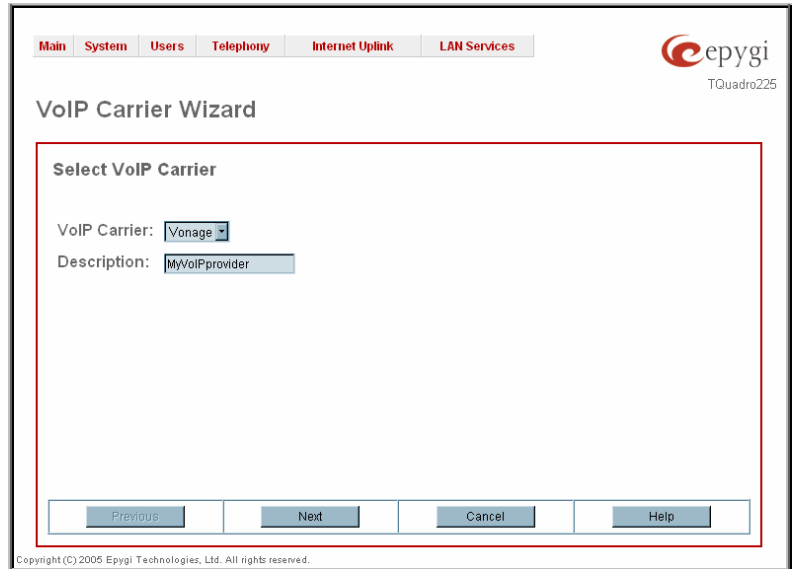


Fig. II-109: VoIP Carrier Wizard page 1

VoIP Carrier Wizard – Page 2 is used to define VoIP Carrier Settings. The page contains following components:

1. VoIP Carrier Common Settings

The **Account Name** text field requires a username for authentication on the defined SIP server.

The **Password** text field requires a password for authentication on the defined SIP server.

The **Confirm Password** text field requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error message “Incorrect Password confirm” will appear.

The **SIP Server** text field requires an IP address or the hostname of the SIP server destination party it is registered on.

The **SIP Server Port** text field requires the port number of the SIP server destination party it is registered on.

2. VoIP Carrier Advanced Settings

The **Use RTP Proxy** checkbox is applicable only when a route is used for calls towards a configured VoIP Carrier from a peer located outside the Quadro. When this checkbox is selected, the RTP streams between external users will be routed through Quadro. When the checkbox is not selected, RTP packets will move directly between peers.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested only for certain SIP servers. For others, the field should be left empty.

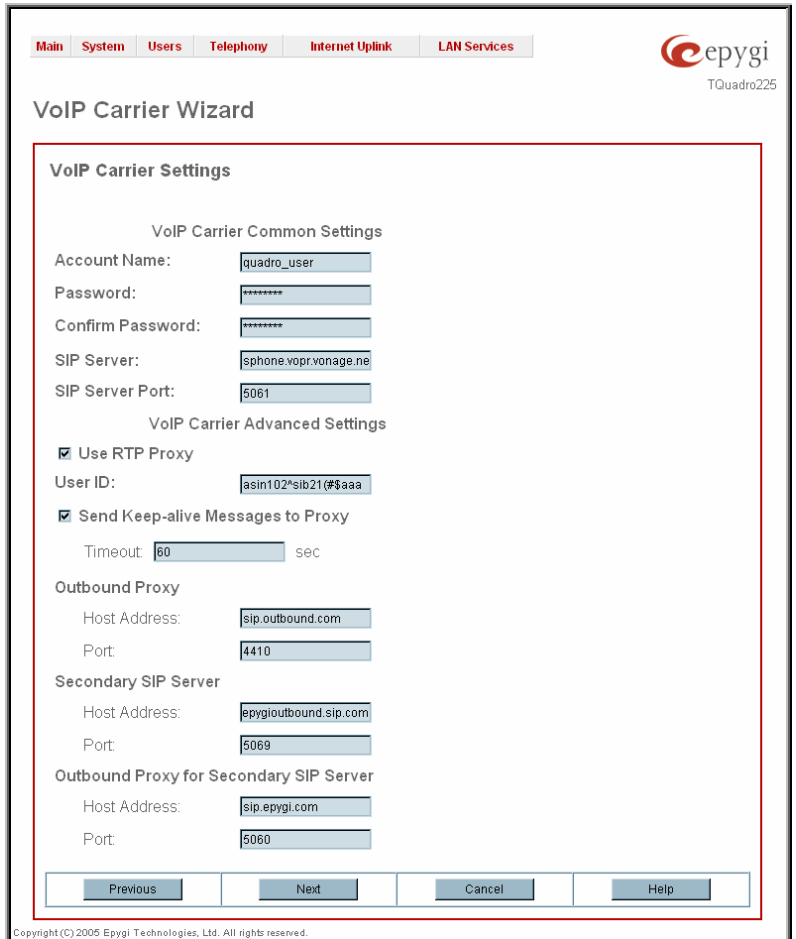


Fig. II-110: VoIP Carrier Wizard page 2

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If a reply is not received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will continue to be sent to the server.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name), the port number of the **Outbound Proxy, Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by Quadro to reach the selected SIP servers.

VoIP Carrier Wizard – Page 3 contains the following VoIP Carrier access code selection components:

The **Access Code** text field requires a digit combination by dialing, which the corresponding VoIP Carrier will be reached.

The **Route Incoming Calls To** drop down list allows you to select an extension (or Auto Attendant) on the Quadro where incoming calls from the configured VoIP Carrier should be routed to.

The **Failover to PSTN** checkbox selection will route the call to the PSTN through local FXO line in case if the VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the [Call Routing](#) table. This maintains digit transmission to the local PSTN when an IP call towards the configured VoIP Carrier cannot be established.

Please Note: A warning message will appear when the defined **Access Code** already exists in the Call Routing table or causes a conflict with entries already in the Call Routing table. In this case, when continuing through the **VoIP Carrier Wizard**, the existing entry in the Call Routing table will automatically be overwritten by the new settings.

Fig. II-111: VoIP Carrier Wizard page 3

RADIUS Client Settings

RADIUS (Remote Authentication Dial In User Service) specifies the RADIUS protocol used for authentication, authorization and accounting, to differentiate, to secure and to account for the users. The RADIUS Server provides the option for a caller from/through Quadro to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the Quadro, and according to the configuration of **AAA Required** option (see [Call Routing](#) table), the RADIUS server will be used to authenticate user and/or to account for the call. This can be accomplished by automatic detection of the caller's number or a customized login prompt where the caller is expected to enter a username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, user passwords are encrypted when sent between the client and RADIUS server to eliminate the possibility of a party viewing an unsecured network where they could determine a user's password. If no response from the RADIUS Server is returned after the Receive Timeout expires, the request is resent numerous times as defined in the Retry Count list. The client can also forward requests to an alternate server(s) if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not recognize must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the Quadro Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the Quadro.

Please Note: The RADIUS Client cannot be disabled if there is at least one route with **RADIUS Authentication and Authorization** or **RADIUS Accounting** values configured in the **AAA Required** drop down list at the [Call Routing](#) table. In order to be able to disable the RADIUS Client on the Quadro, appropriate routes should be removed first.

The other RADIUS Client settings are divided into three groups:

1. Registration Settings

The **Primary Server** requires the IP address of the primary Radius Server.

The **Secondary Server** requires the IP address of the secondary Radius Server.

NAT Station IP text fields require the NAT PC WAN IP address. If no NAT Station is specified here, Quadro's IP address will be sent to the RADIUS server.

Secret Key is used to insert the secret key between the Radius client and the server. Contact the Radius server administrator to get the secret key for your Quadro.

The **Confirm Secret Key** field is used to verify the secret key. If the entered **Secret Key** does not correspond to the one in the **Confirm Secret Key** field, the error message "The Secret Key does not match. Please try again" will appear.

Retry Count allows you to select the number of attempts authorized before canceling the registration.

Receive Timeout allows you to select the timeout (in seconds) between two attempts to register.

Encoding Type allows you to select the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type should also be requested from the Radius Server administrator.

The **Authorization Port** text field requires the port number on the RADIUS server where Quadro is to send the authentication requests.

The **Accounting Port** text field requires the port number on the RADIUS server where Quadro is to send the accounting messages.

2. Authentication Settings

The **Enable common login for all users in time of by Phone authentication** checkbox enables custom settings for the callers who passed an authorization by phone on the Quadro. This checkbox enables **Username** and **Password** text fields to insert the custom settings that will stand instead of the source caller's settings when being delivered to the RADIUS server.

The **Authentication on Destination RADIUS Server** parameters group is used to insert a **Username** and a **Password** (followed by the password confirmation) to pass authentication on the RADIUS Server of the destination Quadro. If these fields are left empty, the original authentication settings that users enter for authentication will be used.

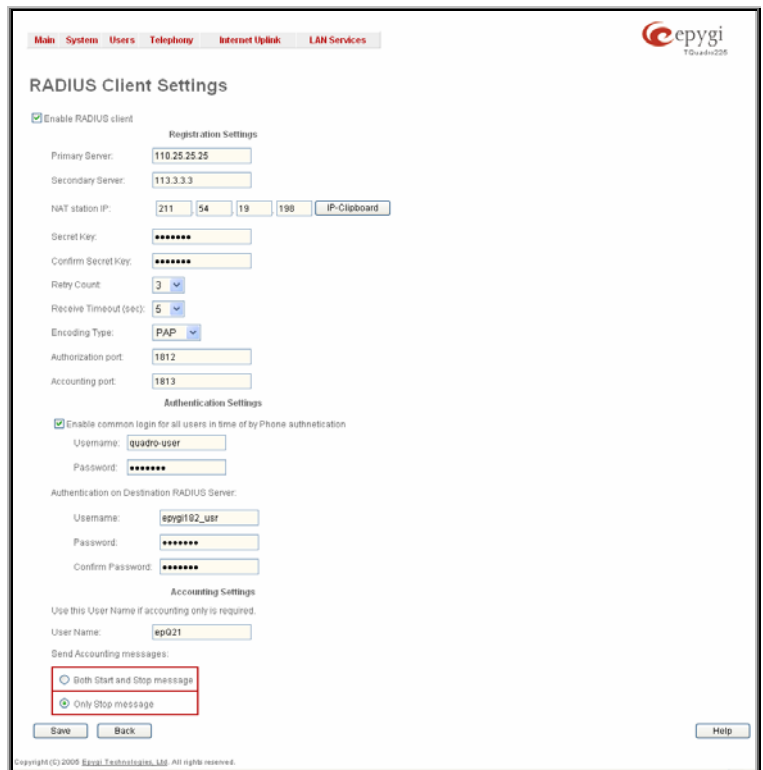


Fig. II-112: Radius Client Settings page

3. Accounting Settings

The **Username** field is dedicated for accounting services only. It is used to insert an identification username for accounting purposes. When no username is specified in this field, the source username will be used for accounting.

The **Send Accounting messages** manipulation radio buttons group is used to select sending both **Start** and **Stop** accounting messages or only **Stop** accounting message.

Dial Plan Settings

The **Dial Plan Settings** page is used to adjust the dialing timeouts for the routing calls over Quadro.

This page consists of the only drop down list used to configure the dialing timeout for the Routing calls. Values selected in the lists indicate the interval between the dialed number and it being applied to the network.

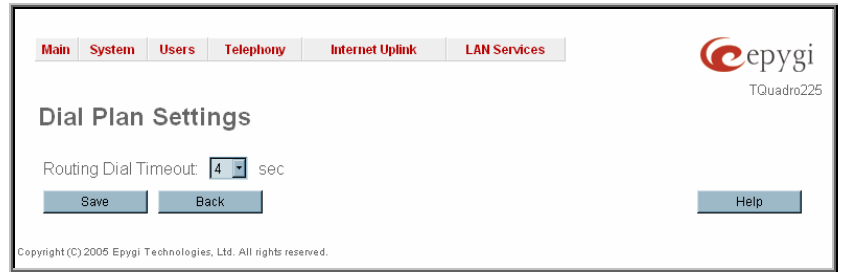


Fig. II-113: Dial Plan Settings page

System Hold Music Settings

The **System Hold Music Settings** allows you to define the hold music played to the PSTN party when it is held by the IP user. This page also allows you to define the percentage of system memory dedicated to the uploaded hold music file. This page contains following components:

The **Play Hold Music** drop down list specifies the music played to the PSTN party when it is held by remote IP user. It offers the following options:

- **Off** - no music will be played.
- **Local Music** – the hold music configured on the Quadro will be sent to the remote PSTN party while it is on hold.
- **Remote Music** – music sent by the IP party will be transparently passed to the PSTN user while it is held by the IP party.

Restore Default Hold Music File enables the default hold music. If the checkbox is selected, the text field **Upload New Hold Music File** will be disabled.

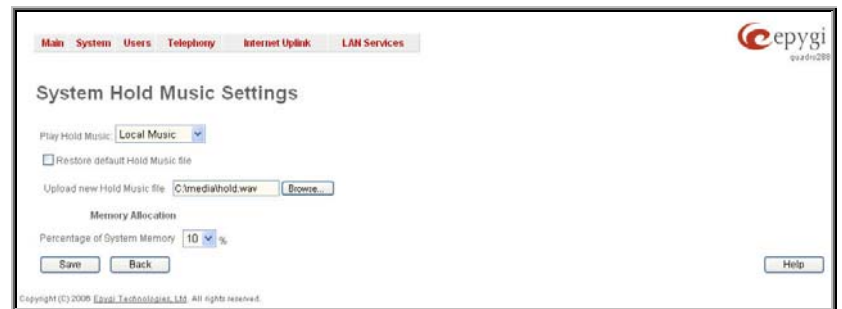


Fig. III-114 Basic Services - Hold Music Settings page

The **Upload New Hold Music File** text field can be used to enter the path where the custom hold music file is located. If the hold music file is browsed with the help of file-chooser, this field displays the path of the browsed file. The **Browse** button is used to browse for the hold music file.

The music file needs to be in PCMU wave format, otherwise the system will prevent uploading the file and will display the warning message "Invalid audio file or format is not supported". Additionally, the system will refuse uploading if insufficient memory is available for the Quadro and will then announce "You do not have enough space".

The **Download Hold Music File** link appears only if a file has been uploaded recently. It downloads the audio file to the PC and opens a window where the saving location can be specified.

The **Percentage of System Memory** drop down list allows you to select the space for the custom hold music. The maximum value in the drop down list is equal to the maximum available space on Quadro.

Internet Uplink Menu



Fig. II-115: Internet Uplink menu in Dynamo theme

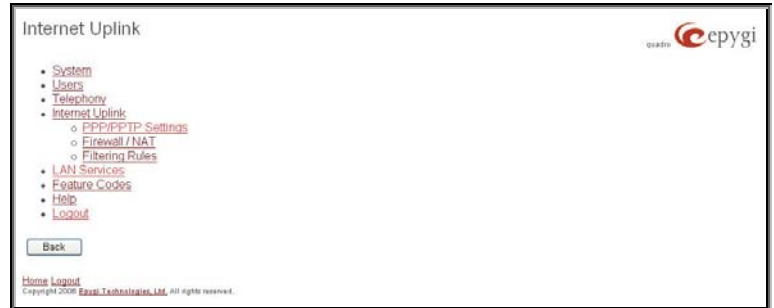


Fig. II-116: Internet Uplink menu in Plain theme

PPP/ PPTP Settings

The **PPP/PPTP Settings** page is used to establish a connection over the DSL link, or any other type of uplink, to the ISP. A connection is needed to set up and make or receive calls through PPP over Ethernet. The connection may be configured for manual setup or always up. Once a connection has been established between the Quadro and the provider, Quadro users will be able to make and receive calls at any time.

The **PPP/PPTP Settings** page offers the following components:

The [Advanced PPP Settings](#) link refers to the same named page where certain parts of the negotiation process during connection establishment can be adjusted. This link is not available when accessing this page through the [Internet Configuration Wizard](#).

The **PPTP Server** text fields are only enabled when Quadro is running with the PPTP interface and require the IP address of the PPTP server.

The **Encryption** drop down list is only enabled when Quadro is running with the PPTP interface and it is used to select the encryption for the traffic over the PPTP interface.

Authentication Settings require the Username and Password used for the authentication on the ISP server.

Dial Behavior radio buttons enables the following selections:

- **Dial Manually** - if this radio button is activated, a button will be displayed in the main management window that serves to switch the Internet connection on/off. When accessing the Internet, every station of the connected LAN has to connect to Quadro first.
- **Always connected** - Quadro stays in the always connected mode. This will allow always being online in the network.

IP Address Assignment radio buttons are used to define the IP address assignment for the PPP interface with the following options:

- **Dynamic IP Address** – the IP address to the PPP interface will be assigned dynamically by the DHCP server.
- **Fixed IP Address** – the fixed user defined IP address will be assigned to the PPP interface.

The **Keep Connection alive** checkbox enables keeping the connection alive by sending control packets dedicated for the link state verification.

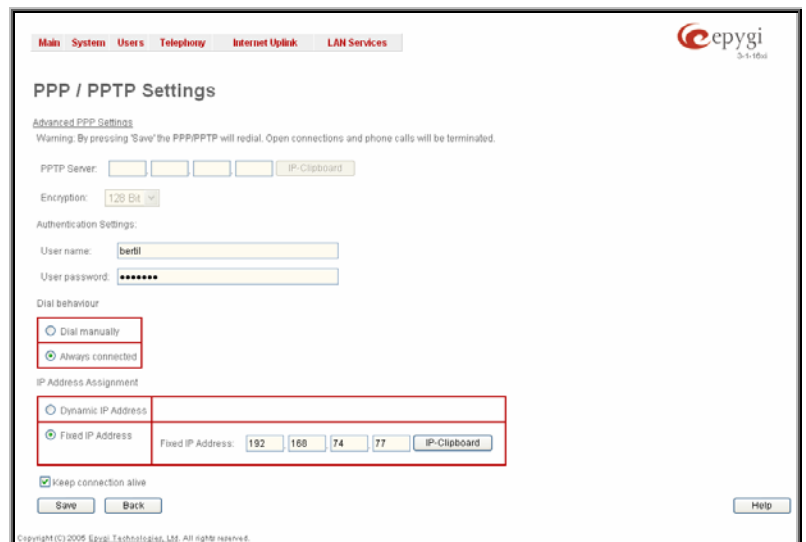


Fig. II-117: PPP Dial Settings page

Advanced PPP Settings

The **Advanced PPP Settings** are used to enable/disable certain parts of the negotiation process during connection establishment. These settings are available only if Quadro has a PPPoE WAN interface.

Attention: Disabling any of the services below may cause problems when establishing a connection including the complete connection failure. The default settings should be changed only if the ISP (Internet Service Provider) specifically requires it or if the peer system has problems with one of the services listed below. More information about these services can be found at: <http://www.protocols.com/pbook/ppp.htm>.

The **Advanced PPP Settings** page offers the following group of checkboxes:

Enable automatic PPP restart at checkbox is used to select the time when the PPP connection will automatically be restarted. The checkbox selection enables **LCP echo failures** text field that indicates the number of the LCP echo failure packets received before the PPP connection will be considered as dead and will be restarted.

Disable CCP (Compression Control Protocol) negotiation - this option should only be selected if the peer system is not working properly. For example, if it is not accepting the requests from the PPPD (Point-to-Point Daemon) for CCP negotiation.

Disable magic number negotiation - with this option, PPPD cannot detect a looped-back line. This option should only be selected if the peer is not working properly.

Disable protocol field compression negotiation in both the receive and the transmit direction – with this option, no protocol field compression will take place.

Disable Van Jacobson style TCP/IP header compression in both the transmit and the receive direction – with this option, no negotiation of TCP/IP header compression will take place and the header will always be sent uncompressed.

Disable the connection-ID compression option in Van Jacobson style TCP/IP header compression - with this option, PPPD will not compress the connection-ID byte from Van Jacobson and will not ask the peer to do so.

Disable the IPXCP and IPX protocols - this option should only be selected if the peer is not working properly and cannot handle requests from PPPD for IPXCP negotiation.

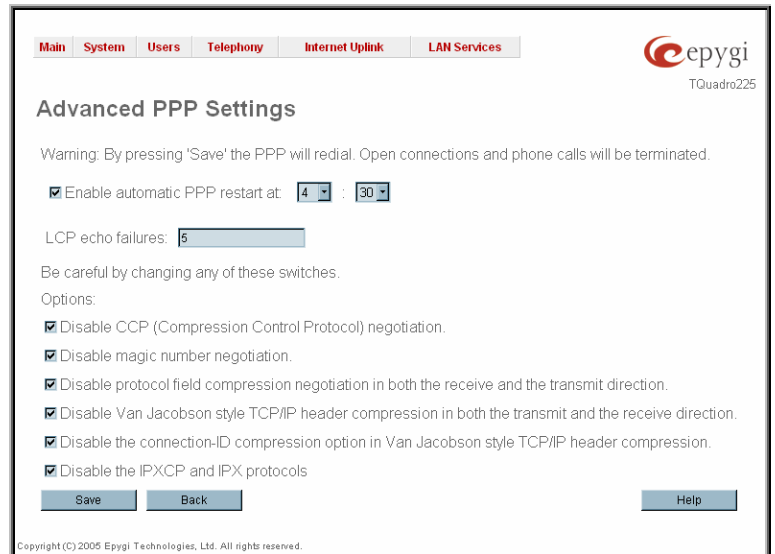


Fig. II-118: Advanced PPP Settings page

Firewall and NAT

The **Firewall Configuration** page allows setting up a firewall, configuring the security level and enabling the NAT and IDS services of Quadro.

A **Firewall** is a security service configured by the Quadro administrator based on various criteria. The firewall allows or blocks traffic based on policies, services and/or IP addresses. The firewall has several levels of security policies (low, medium or high). The administrator may add additional service-based rules. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level.

NAT (Network Address Translation) is used to allow Quadro LAN members to connect to the Internet using Quadro's WAN IP address. The Quadro/NAT also handles forwarding incoming packets from the WAN to the PCs or devices on Quadro's LAN.

The **Firewall Configuration** page offers the following components:

The **Enable NAT** checkbox selection enables Network Address Translation.

The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are the following:

- **Low Security** - Everything that is not explicitly forbidden will be allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

The [Advanced Firewall Settings](#) link refers to the page where Quadro's privacy can be configured.

The [View Filter Rules](#) link opens the [Filtering Rules](#) page.

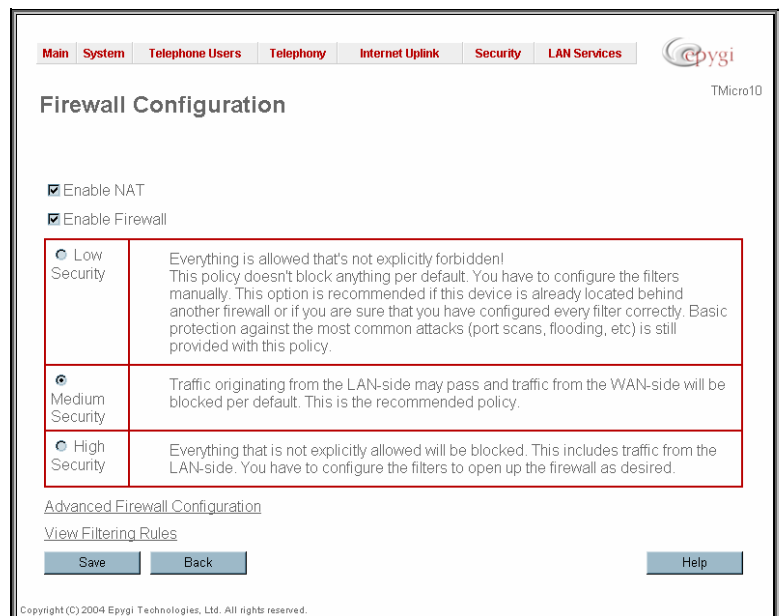


Fig. II-119: Firewall and NAT Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping and Portscanning operations addressed towards the device. With these features enabled, Quadro will answer with inscrutable messages to the Ping and Portscanning operations.

Please Note: Operations are available only when the firewall is enabled from the [Firewall and NAT](#) page.

This page offers the following components:

The **Ping Stealth** checkbox selection prohibits a Ping operation toward Quadro from its WAN.

The **Fool Portscanner** checkbox selection prohibits Quadro portscanning from its WAN. As a reply to a Portscanning operation, "network unreachable" or "host unreachable" feedback messages will be sent.

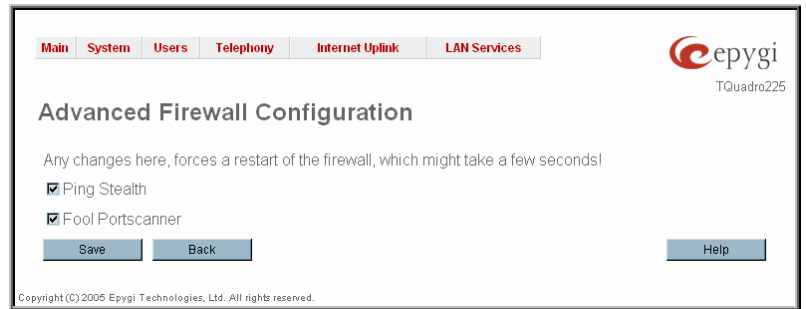


Fig. II-120: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows you to configure the filters for incoming and outgoing traffic.

To prevent inaccurate configuration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. Since the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled (additionally NAT should be enabled to use the **Port Forwarding** function in the **Incoming Traffic / Port Forwarding** filtering rules). The filtering rules are independent from the security level, so they will work if enabled, no matter what security level has been selected.

Please Note: Applying firewall rules will prevent the establishment of new connections that violate the rules. Applying rules does not kill existing connections that violate the rule.

View All displays all configured filters specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). Since it is read-only, no modifications are allowed and no functional buttons are available.

The **Incoming Traffic/Port Forwarding** filter is for incoming traffic. The rules here allow or deny systems on the Internet to reach the services of Quadro's LAN. The NAT service should be enabled on the Quadro to provide the possibility of **Port Forwarding** in the **Incoming Traffic/Port Forwarding** filtering rules. The **Port Forwarding** function will be unavailable if NAT is disabled on the Quadro.

The **Outgoing Traffic** filter is for outgoing traffic. The rules here allow or deny Quadro's LAN users to reach external services.

Management Access is used to enable management access to the Quadro from the Internet. A host on the Internet can be allowed to reach the Quadro.

SIP Access is to allow or deny the SIP access to or from the particular SIP servers, SIP hosts or a group of them. The **SIP Access** filtering rule may prevent or allow incoming or outgoing SIP calls to or from specified SIP server(s) or host(s).

H323 Access is to allow or deny the H323 access to or from the particular H323 servers, H323 hosts or a group of them. The **H323 Access** filtering rule may prevent or allow incoming or outgoing H323 calls to or from specified H323 server(s) or host(s).

When **Blocked IP List** is used, traffic from specific hosts may be blocked, no matter what services are opened in the other filters. NO traffic will be allowed to the specified hosts. The **Blocked IP List** service has a higher priority if the same host is also listed in the **Allowed IP List** table.

Allowed IP List allows trusted hosts to reach your network and vice versa. It is an exception to other rules and only all services may be allowed for a single host.

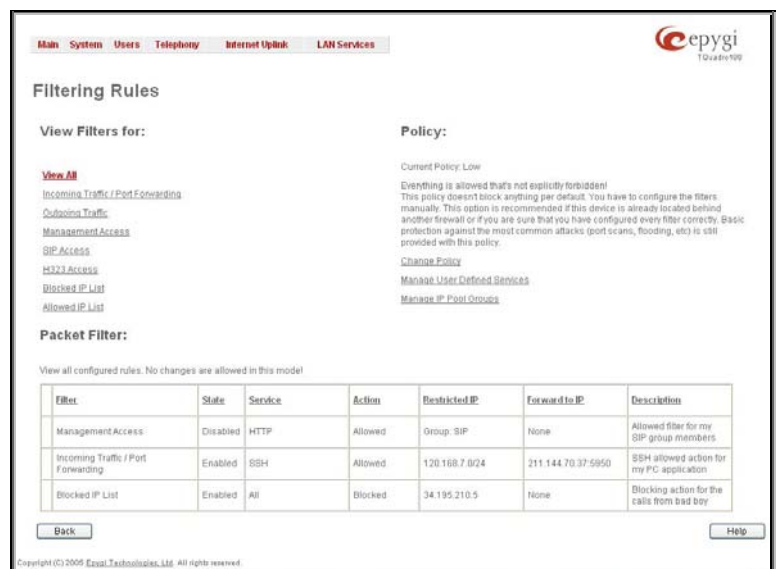


Fig. II-121: Filtering Rules page

The **Filtering Rules** page provides several links. Each link opens its specific parameters on the same page. Only **Change Policy** (see chapter [Firewall and NAT](#)), **Manage user Defined Services** (see chapter [Service Pool](#)) and **Manage IP Pool Groups** (see chapter [IP Pool](#)) lead to separate pages. The **Filtering Rules** page also includes the currently selected firewall security (**Policy**) level and its description.

The table displayed on the bottom of this page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**) and the destination of port forwarding (**Redirect to**, in case of **Incoming Traffic/Port Forwarding**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Disable** is used to disable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action**, a **Restriction** to certain IP address(es) or IP groups, and if adding a rule for **Incoming Traffic/Port Forwarding**, the destination IP address for **Forwarding**.

The page to add a rule for **Incoming Traffic/Port Forwarding** offers the following input options:

Service includes a list of possible services to be configured. All user-defined services also will be displayed in this list.

Action includes possible actions to setup the rule.

Forward to IP requires the destination IP address where traffic should be transferred to if it comes from the restricted host. The IP address defined in this field will be ignored for blocked action of the **Incoming Traffic/Port Forwarding** rule.

Note: It is not allowed to forward incoming packets when the NAT service is disabled on the Quadro.

Port Translation text field is available for "Allowed" action only and optionally requires the port number that will stand instead of the original port number when incoming packet is being forwarded. If this field is left empty, the original port number will be used when forwarding the packet.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.
- Selecting **Single IP** will require the IP address of the allowed or blocked host.
- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. The following are **Maskbit** examples:
 255.0.0.0 = /8,
 255.255.0.0 = /16,
 255.255.255.0 = /24,
 255.255.255.255 = /32
- **Group** indicates the user-defined groups that include IP addresses that should be allowed or blocked.

The **Description** field is used to insert an optional description of the filtering rule.

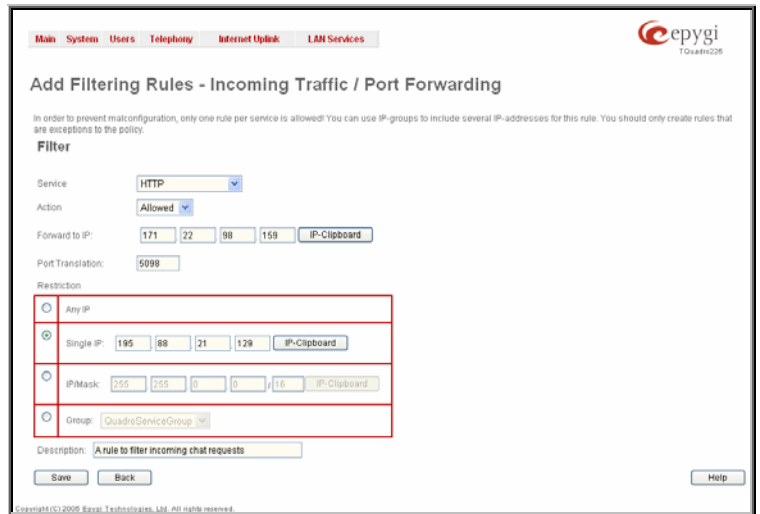


Fig. II-122: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filter** link (Incoming Traffic/Port Forwarding, Outgoing Traffic, Management Access, SIP Access, H323 Access, Blocked IP List, Allowed IP List) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the **Filtering Rules** page. A page where a new rule may be added will appear in the browser window. The page will be named corresponding to the selected filter.
3. Select a service name from the **Service** list to configure a rule for it. If the list has a default value, do not change the default values.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, do not change the default values.
5. Enter the IP address in the **Forward to IP** field if an **Incoming Traffic Rule** is to be added.
6. Choose the restriction type by selecting **Any**, **SingleIP** or **IP/Mask** and enter the required information in the text fields or select a group.
7. Insert a **Description**, if needed.
8. To add a rule with these parameters, press **Save**.

To Delete Filtering Rules

1. Select the **Filter** link to delete a rule from its table. The appropriate **Filter** table will appear in the same window.
2. Check one or more checkboxes of the corresponding rules that should be deleted from the rules table. Press **Select all** if all rules should be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

Service Pool

The **Service Pool** table is a list of all created services and their parameters. It is used to add new services with the appropriate settings (protocol type and port range). New services can be used to add a restriction or permission by defining a new filtering rule with the following:

Add opens the **Add New Service** page where new services may be added.

Edit opens the **Edit Service** page where the service parameters (except for the service name) can be modified. This page includes the same components as the **Add New Service** page. To operate with **Edit** only one record may be selected, otherwise the error message "One row must be selected" will appear.

The **Add** page is used to add new services and includes the following text fields and buttons:.

Service Name requires a name for the service that should be added.

Protocol includes a list of possible protocols to be selected.

Port Range requires a port range for the defined service.

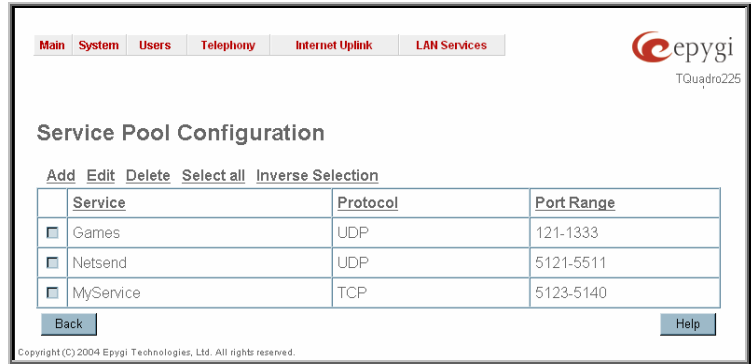


Fig. II-123: Service Pool page

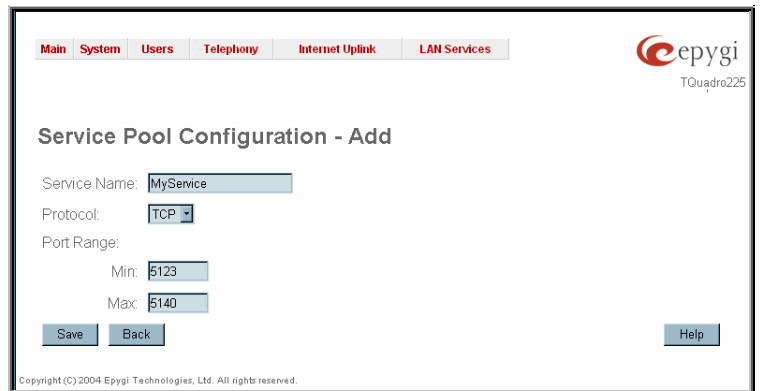


Fig. II-124: Service Pool - Page to add a new Service

To Add a new Service

1. Select the **Manage User Defined Services** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **Service Pool Configuration** page. A page where a new service may be added will appear in the browser window.
3. Define a service name in the **Service Name** text field.
4. Select the protocol type for the service from the **Protocol** drop down list.
5. Enter the port range in the **Port Range** text fields or leave one of them empty to define a particular port for the service.
6. To add a service with these parameters click on **Save**.

To Delete a Service

1. Select the **Manage User Defined Services** link. The **Service Pool Configuration** page appears with the table of services (if any).
2. Check one or more checkboxes of the corresponding services that should be deleted from the **Service Pool** table. Press **Select all** if all services should be deleted.
3. Click on the **Delete** button on the **Service Pool Configuration** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

IP Pool

The **Manage IP Pool Groups** link opens the **IP Pool Configuration** page.

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.



Fig. II-125: IP Pool Configuration page

Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains).

Clicking on the **Group** name will display an **IP Pool Group Configuration** page with the **Members** list for the current group.



Fig. II-126: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.



Fig. II-127: IP Pool Group Configuration page

The **Add Members** page provides the following radio buttons:

IP address requires the member IP address that is to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

The **User-defined Group** includes previously added groups that may also be added as a member to another group.

Member description text fields can be used to enter an optional description of the member.

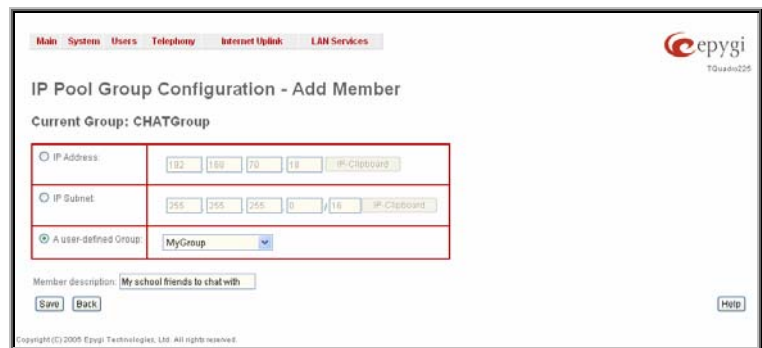


Fig. II-128: IP Pool Group Configuration – Add Member

To Add a new Group with Members

1. Select the **Manage IP Pool Groups** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **IP Pool Configuration** page. A page where a new group may be added will appear in the browser window.
3. Define a group name in the **Group Name** text field and fill in the **Group Description**, if needed.
4. To add a group with the given parameters, press **Save**.
5. Open the **IP Pool Group Configuration** page by clicking on the group name.
6. Select the **Add** button on the **IP Pool Group Configuration** page. A page opens where new members may be added to the group.
7. Enter an IP address for the member in the **IP Address** text fields, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
8. Enter a **Member Description** in the corresponding text field, if needed.
9. To add a member with these parameters to the selected group press **Save**.

To Delete a Member

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Click on the desired members that should be deleted. The **IP Pool Group Configuration** list will appear.
3. Check one or more checkboxes of the corresponding members that should be deleted from the **Members** table. Press **Select all** if all members should be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.
5. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

To Delete a Group

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Check the one or more checkboxes of the corresponding groups that should be deleted from the groups table. Press **Select all** if all groups should be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

LAN Services Menu

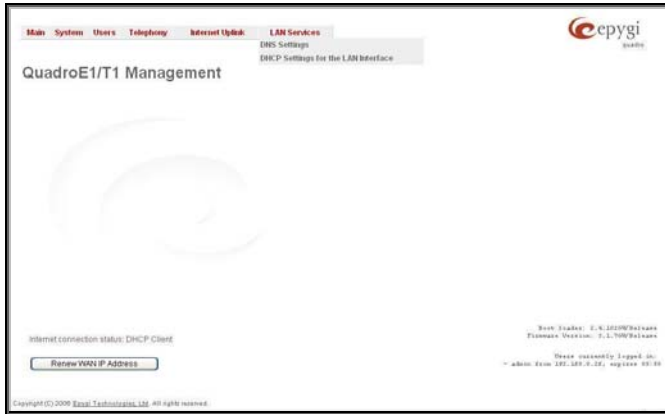


Fig. II-129: LAN Services menu in Dynamo theme



Fig. II-130: LAN Services menu in Plain theme

DNS Settings

The **DNS Settings** page provides the option of setting up a name server for the Quadro. It offers the following components:

The **Nameserver Assignment** radio buttons are as follows:

- The **Dynamically by provider** selection automatically configures the assignment of the name server address from the provider party.
- **Fixed Nameserver address** is a manually selected name server. The **Nameserver** text field requires the IP address of an external name server. The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.

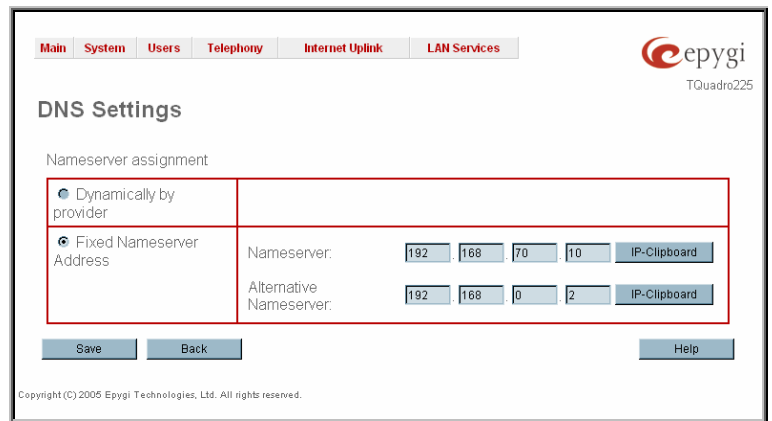


Fig. II-131: DNS Settings page

DHCP Settings for the LAN Interface

The **DHCP Settings** page provides the option of enabling a DHCP server and controlling the Quadro user's LAN settings. Therefore, Quadro LAN users will automatically be provided with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the Quadro's IP address)
- WINS server
- Nameserver (corresponds to the Quadro's IP address)
- Domain name

The **DHCP Settings** page offers the following input options:

Enable DHCP Server activates the DHCP server on Quadro.

IP Address Range defines a range of IP addresses that will be assigned to the Quadro LAN users. The IP range must be at least 6, otherwise the error message "Address Range too small" will prevent it from being saved. The error message "Address Range too large" will appear if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the Quadro LAN users.

View DHCP Leases leads to the page where the DHCP leased LAN IP addresses are listed.

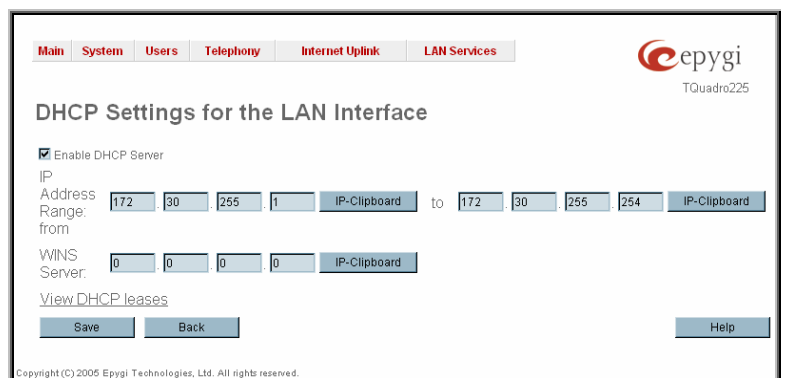


Fig. II-132: DHCP Settings page for LAN interface

The **DHCP Leased IP Addresses** page includes a list of the leased host addresses that are part of the Quadro's LAN. For these hosts, Quadro acts as a server supplying them with a unique IP address. It displays a read-only table describing all the leased IP hosts and their parameters. The table contains the following columns:

IP address - host IP address, assigned by Quadro.

MAC address - host MAC address, provided by the host itself.

Lease Start - date and time when the leased IP address has been activated.

Lease End - date and time when the leased IP address has been or will be deactivated.

Hostname - hostname, provided by the host itself.

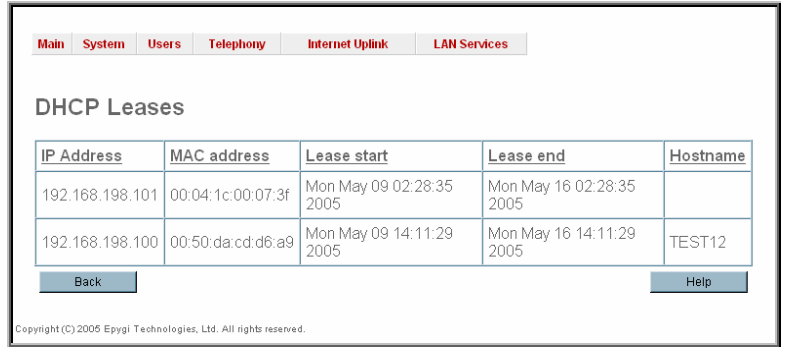


Fig. II-133: DHCP Leases page for LAN interface

Registration Form

The **Registration Form** page appears when administrating an unregistered Quadro, and it has been created for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It provides several links offering the following registration options:

Register now leads to the Epygi Technical Support System Registration page and requires customer's information to submit the Quadro registration form.

Remind me later hides the registration notification in the Quadro through [System Configuration Wizard](#) or [Internet Configuration Wizard](#) until the next administrating activities..

Don't remind me more hides the registration notification forever.

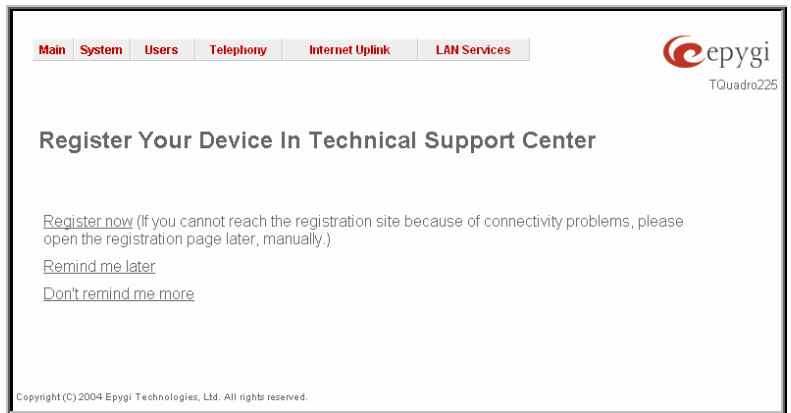


Fig. II-134: Device Registration page

Logout

This option is used to close the session between the user PC and Quadro and to leave the Quadro Web Management or to enter the management with another login. By selecting the **Logout** button, the startup page will be displayed and the user needs to login again.

QuadroE1/T1's Feature Codes

This chapter describes Quadro's call codes enabling the user to navigate through Quadro's services with the help of a phone handset. These services are **Establishing a Call** and **PBX Services**.

Establishing a call

To make a call, dial the **Routing Number**.

Routing Numbers and available routs to, from and through Quadro are listed in the **Local Routing Table**, which is configured and managed by Quadro's Administrator. To get information about dialing rules, please turn to administrator.

Please Note: You may accelerate establishing a connection by a pound (#) sign dialed at the end of the number.

Using Quadro's PBX Services

PBX Services accessible at the dial tone, characterized by beginning with the key *.

Administrator Login Allows you to modify the auto attendant (AA) greeting.	* 7 5
--------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Administrator Login

At the moment, the administrator login allows only the modification of the auto attendant (AA) messages:

* 7 5 Administrator's Login	
1 Auto Attendant Welcome Message	2 Auto Attendant Menu Message
1 Listen to Current AA Welcome Message	1 Listen to Current AA Menu Message
2 Record a New AA Welcome Message	2 Record a New AA Menu e Message
3 Restore Default AA Welcome Message	3 Restore Default AA Menu Message
# Stop Recording or Playback	
* 0 Administrator's Logout	

After dialing * 7 5, use key 1 to enter the auto attendant regular greeting menu and use key 2 to enter the auto attendant menu message. The key combinations beside are available to modify the auto attendant greetings.

QuadroE1/T1's Auto Attendant Services

Quadro's Auto Attendant is addressed to provide remote access to the Quadro voice connectivity services. Specifically it supports remote connection to Quadro extensions, their mailboxes and making pass-through calls to other destinations. Remote access to the Quadro auto attendant is possible through IP and PSTN calls.

Quadro's Auto Attendant can be accessed locally, remotely from the IP network (by dialing Auto Attendant's SIP address) and from the PSTN network (by dialing Quadro's PSTN number) if the calls addressed to the Quadro's PSTN number are routed to the Auto Attendant.

Attention: If the Auto Attendant authentication attempts have been failed for the five times, Quadro's Auto Attendant will become unavailable for the next 5 minutes.

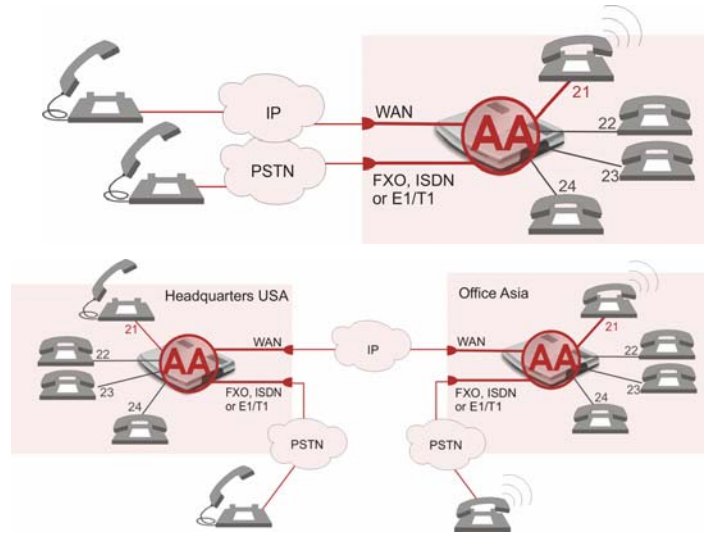
The automated attendant services are divided into 2 feature groups: **Connection Service** is supported by the voice messages help which helps caller to navigate within area using the handset buttons. **Call Relay** service is available using the appropriate call code, but is not supported by voice messages. Thus, it is hidden for external callers.

Connection Service provides access to all extensions of the Quadro device without restrictions: All Quadro extensions may call each other dialing the extension number. And all external callers (using PSTN or IP calling) can reach every Quadro extension dialing Quadro's phone number and using the Auto Attendant's voice menu to be connected to the desired extension by entering the extension number.

Call Relay

As the Quadro Auto Attendant is registered at Epygi's SIP server by default, it may be used as a kind of private switching center, if the Auto Attendant is routed to the particular telephone line (FXO, ISDN or E1/T1) as a "default user". Then it allows e.g. establishing cost-saving long-distance calls: Via PSTN to the Quadro Auto Attendant (e.g. USA headquarters), via IP to the remote Quadro Auto Attendant (e.g. Office Asia) and via PSTN to the desired destination (see call codes below).

Access to **Call Relay** needs authorization.



Call Codes Available in Auto Attendant

For external IP calls addressed to the Auto Attendant or incoming calls from mainline routed to the Auto Attendant or local by dialing the 2-digit attendant extension, following key combinations are available to access and manipulate within Auto Attendant services:

Incoming call to Auto Attendant Services or dial locally	Keys
Extensions Menu - establishing a connection to an extension on the called Quadro	- (already in)
<p>Call Relay Menu - mainly for external calls (IP/FXO or IP/ISDN) but local calls are also allowed.</p> <p>This service avoids having to hang up and redo the entire dialing process if Quadro detects an error in the dialed number or the user decides to cancel the call and dial a new number. By entering the combination * * the call will be interrupted and the user will get an invitation to dial a new one. This is applicable during dialing, after the ring tone has started, and after the call has been established.</p> <p>* * digit combination is applicable:</p> <ul style="list-style-type: none"> • During the dialing, • After ring tones start, • After call establishment. <p>Under the following restrictions:</p> <ul style="list-style-type: none"> • This feature can be used when accessing the AA from the PSTN line to make IP or local calls • This feature can be used when calling to the PSTN through the AA • This feature is not available on the second Quadro Auto Attendant (calling from one Auto Attendant to another) 	* 2
Non-Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to change the callback destination for a one-time callback. After the caller hangs up, Quadro will call back to the newly specified number. This change will not be logged into Authorized Phones Database.	* 5
Permanent Call Back – allows PSTN callers registered in the Authorized Phones Database to reconfigure Authorized Phones Database entries by modifying the caller's and/or callback numbers. The caller will then be able to initiate a callback only by calling from the newly specified caller number.	* 6
Call Routing Management Menu – allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry.	* 7
Quits the Auto Attendant and starts a dial tone.	Flash 4

Appendix: System Default Settings

Parameter	System Default Value
Admin Settings	Login name -admin Password - 19
Quadro Hostname	quadro
LAN IP Address	172.30.0.1 Subnet Mask - 255.255.0.0
DHCP Server	Enabled, IP Range - 172.30.0.100-172.30.0.254, WINS - 0.0.0.0.
Regional Settings and Preferences	Locale – US, TimerZone - US/Central, Theme – Dynamo.
WAN Interface Protocol	Ethernet
WAN Interface Bandwidth	Upstream – 10000, Downstream – 10000, Min Data Rate – 0.
WAN IP	Automatically through DHCP
Mac Address	Assigned by device, MTU - 1500 Bytes.
DNS Server	Dynamically
IP Routing Configuration	No Routes
Event Settings	"Display notification" for all except Login event, which has "Do nothing" action assigned.
Time/Date Settings	NTP Server and Client – enabled, Predefined NTP Server - ntp1.epygi.com, Polling interval – 6.
Mail Settings	Disabled
SNMP Settings	SNMP - Enabled, System Location and System Contact - undefined, SNMP v1 / 2c – enabled SNMP v1 / v2c Read-Only Community – public SNMP v1 / 2c Read-Write Access – disabled No SNMP traps defined
Language Pack	Default - English Custom Language Pack - none
User Rights Management	Users - admin (enabled), localadmin (disabled). Roles - Local Administrators (all accessible pages for localadmin).
Extensions Management	00 and 11 extensions exist
Extension Settings – General	Display name – none, Password – empty, Attached to the FXS line 1, Call Relay – disabled, External Call Policy – disabled.
Extension Settings – SIP	Registration username and password - automatically generated, SIP server - sip.epygi.com, SIP Server port – 5060, SIP Server Registration – enabled.
Extension Settings – SIP Advanced	Authentication User Name – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined.
Extension Settings – H.323	Disabled
Extension Settings – H.323 Advanced	User ID – undefined, Address, Port and Dial Access Port – undefined.

Parameter	System Default Value
Extension Settings – Codecs	Codecs - G711u (preferred), G711a, G729a, G726/32, G726/16, G726/24, G726/40 Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Attendant 00 Settings – General	Display name – Attendant.
Attendant 00 Settings – Attendant Scenario	Scenario – default, Send AA digits to Routing Table – disabled, Redirection on Timeout – disabled, Welcome message – enabled, Welcome message and Recurring Attendant Prompt – default, Attendant Ringing Announcement – disabled, Authorized Phones Database – undefined.
Attendant 00 Settings – SIP and SIP Advanced	Same as for an extension.
Attendant 00 Settings – H.323 and H.323 Advanced	Same as for an extension.
Attendant 00 Settings - Codecs	Codecs - G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, G723, iLBC Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls - disabled.
Call Statistics	Enabled 100 entries for all type of calls
SIP Settings	UDP and TCP Port – 5060, Session Timer – disabled, DNS Server for SIP – default, SIP timers – RFC 3261.
H.323 Settings	UDP port – 1719, TCP Min port – 1720, TCP Max port – 1752, Fast connect – enabled, Tunneling – disabled, TCP connect timer – disabled, Setup timeout – 4 seconds.
RTP Settings	Properties for all Codecs except G723 and iLBC: Packetization -20ms Silence Suppression -yes G723 and iLBC properties: Packetization - 30ms Silence Suppression – yes RTP/RTCP port range - 6000-6099 G276 Standard - ITU-T specification Telephone Event Draft Support - enabled RTCP Support - disabled
NAT Traversal Settings	NAT Traversal for SIP – force NAT Traversal for H.323 – disabled SIP, H.323 and RTP Parameters - Use STUN SIP TCP Port – 5060 H.323 mapped ports – 1720 - 1752 STUN Parameters: Primary STUN Server - stun.ipygi.com Primary STUN Port – 3478 Secondary STUN Server – undefined Secondary STUN Port - undefined Polling Interval: 1 hour Keep-alive interval: 120 seconds NAT IP checking interval: 300 seconds No entries in NAT Exclusion table

Parameter	System Default Value
Line Settings	Onboard Lines Configuration: CallerID- Standard 2 FSK Busy Tone indications: disabled Ringer type: Type A Off-hook caller ID - disabled Loopback Settings – disabled, timeout is 30.
E1/T1 Settings	Trunk0 exists Trunk mode - T1 Interface Type - Network Signaling - CCS Line Code - B8ZS Frame Mode - ESF Line Build Out - short_110-ft Coding - u-law LoopBack Mode - No_loopback Clock Mode – Master TEI mode – non automat, TEI address -0 Alternative Disconnect Mode - enabled Excessive Ack. Delay T200 - 4000 Idle Timer T203 – 10000 T302 timer – 4000 T309 timer – 0 T309 timer – 60000 No Answer Disconnect Timer - 0 D Channel Timeslot for Transmit/Receive - 24 B channels - 1-23 timeslots are enabled, Echo - Cancellation enabled for all B channels Channels Selection – preferred Channels Selection Ordering – ascending Bearer Establishment Procedure – on progress indication with in-band information Called Party Type of Number and Calling Party Type of Number - unknown Called Party Numbering Plan and Calling Party Numbering Plan – ISDN/telephony numbering plan Route Incoming Call to - 00 Switch Type - primary_dss1 Incoming Called Digits Size - 1 Generate Progress Tone to IP – disabled Generate Progress Tone to PSTN/PBX – enabled Enable CLIR Service - disabled
Gain Control Settings	FXS lines: Transmit Gain: - 6 Receive Gain: 0 E1/T1 Trunks: Transmit Gain: 0 Receive Gain: 0
Call Routing	Route all incoming SIP calls to Call Routing – disabled Route all incoming H.323 calls to Call Routing - disabled Local Routing table – no entries. Local AAA Table - no entries.
RADIUS Client Settings	Disabled
Dial Timeouts	4 seconds
System Hold Music Settings	Play Hold Music – Local Music, Hold Music file – default, Percentage of System Memory – 1%.
Firewall	Enabled, Medium level, Ping Stealth - enabled Fool Portscanner - disabled
NAT	Enabled
Filtering Rules	Outgoing Traffic - MS File Sharing (Blocked for all), SIP Access (Allowed for all), No user defined services and IP pool groups

Appendix: Glossary

A

Asymmetric Digital Subscriber Line (ADSL) - is a method for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. An ADSL circuit must be configured to connect two specific locations, similar to a leased line. A commonly discussed configuration of ADSL would allow a subscriber to receive data (download) at speeds of up to 1.544 Megabits per second, and to send (upload) data at speeds of 128 kilobits per second. Thus the 'Asymmetric' part of the acronym. Another commonly discussed configuration would be symmetrical: 384 kilobits per second in both directions. In theory ADSL allows download speeds of up to 9 megabits per second and upload speeds of up to 640 kilobits per second. ADSL is often discussed as an alternative to ISDN, allowing higher speeds in cases where the connection is always to the same place.

Asynchronous Transfer Mode (ATM) - a 53-byte cell-switching technology well suited for carrying voice, data, and video traffic on the same infrastructure. It is inherently scalable in throughput and was designed to provide Quality of Service (QoS).

Auto Attendant (AA) - a feature providing remote access to Quadro voice connectivity services. Specifically, it supports remote connection to Quadro extensions, to their mailboxes and for making calls to other destinations. Remote access to Quadro AA is possible through IP and PSTN calls.

Auto Redial - a service that allows automatically recalling the destination that was busy.

C

Call - establishment of (or attempt to establish) a voice or data connection between two endpoints, or between two points that provide a partial link (e.g., a trunk) between two endpoints.

Call Blocking - a Quadro service that allows blocking unwanted incoming or outgoing calls over Quadro.

Call Forwarding - a Quadro service that allows transferring a call to another destination in case the Quadro user is busy, not answering or unconditional.

Call Hold - a Quadro service that allows holding the call in order to make another one, or to answer the second incoming call. The first call partner will listen to music while being on hold.

Call Waiting - a Quadro service that allows receiving a second call while being busy with the first one. The waiting party will hear a beeping during the conversation.

Caller ID - caller information is displayed on the called party's phone.

Central Office (CO) - a local switching system that connects lines to lines and lines to trunks. Sometimes used to refer to the building in which a switching system is located and the associated equipment. It is also the physical point where calls enter the long distance network.

CODEC - COmpression/DECompression that transforms analog voice into a digital bit stream and vice-versa. It is now an overall term for the technology used in digital audio and video.

D

D-channel - In ISDN, the 16-kb/s segment of a 144-kb/s, full-duplex subscriber service channel that is subdivided into 2B+D channels, i.e., into two 64-kb/s clear channels and one 16-kb/s channel for the ISDN basic rate. **Note 1:** The D channel is usually used for out-of-band signaling. The two 64-kb/s clear channels are used for subscriber voice and data services. **Note 2:** The D-channel specifications are addressed in the CCITT Recommendation for the Integrated Services Digital Network (ISDN). **Note 3:** The D-channel may be 64 kb/s for the primary rate ISDN service.

Data Encryption Standard (DES) - a block cipher algorithm for encrypting (coding) data so it is nearly impossible for anyone without the decryption key to get the data back in unscrambled form. The DES standard enciphers and decipheres data using a 64-bit key.

Dial peer - an addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

Dial plan - a description of the dialing arrangements for customer use on a network.

Digital Signal Processor (DSP) - A specialized microprocessor that performs calculations on digitized signals that were originally analog, and then forwards the results. The big advantage of DSPs lies in their programmability. DSPs can be used to compress voice signals to as little as 4,800 bps. DSPs are an integral part of all voice processing systems and fax machines.

Digital Subscriber Line (DSL) - public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Since most DSL technologies do not use the entire bandwidth of the twisted pair, there remains room for a voice channel.

Distinctive Ringing - Quadro service that allows a specific ringing pattern assignment for particular callers over Quadro.

Domain - a place on the Internet you can visit with your browser, i.e., a www site. It also might be a single computer or computers masqueraded as a single computer. On the Internet, the domain is the address that gets you there.

Domain name - in a network using the TCP/IP, the full domain name consists of a sequence of names (labels) separated by periods (dots), for example, Quadro.epygi.com.

Domain Name System (DNS) - a system used on the Internet for translating names of network nodes into their addresses.

Downstream - in communications, there are two circuits. One coming toward you and the other going away from you. Downstream is another term for the transmission coming toward you.

Dual-Tone Multifrequency (DTMF) - a method of signaling consisting of a push-button or touch tone dial that sends out a sound consisting of two discrete tones that are picked up and interpreted by telephone switches (either PBXs or central offices).

Dynamic Host Configuration Protocol (DHCP) - a network standard regulating the IP address and other information assigned to the clients by the server.

Dynamic Host Control Protocol (DHCP) - a protocol that is used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention.

E

E1 - wide area network digital transmission scheme. E1 is the European equivalent of a T1 line. The E1's higher clock rate (2.048 MHz) allows for 32 separate 64Kbps channels, which include one channel for framing and one channel for D-channel information.

Ethernet - a local area network used for connecting computers, printers, workstations, terminals, servers, etc., within the same building or campus. Ethernet operates over twisted pair and/or over coaxial cable at speed up to 10Mbps.

Ethernet Controller - the unit that connects a device to the Ethernet cable.

Ethernet Switch - the device that connects local area networks.

Extensions - users over Quadro.

External User - users connecting Quadro by IP or PSTN calls.

F

Firewall - a combination of hardware and software that limits the exposure of a computer or group of computers to an attack from outside. A firewall is a system or combination of systems that enforce a boundary between two or more networks. One purpose of an Internet firewall is to provide a single point of entry where a defense can be implemented, allowing access to the Internet resources from within the organization, and providing controlled access from the internet to hosts inside the organization's internal networks.

Firmware - is computer or OS required software that resides on ROM

Foreign Exchange (FX) - a Central Office trunk that has access to a distant Central Office. A dial tone is returned from that distant Central Office and a location can be reached in the area of the foreign Central Office by dialing a local number.

Foreign Exchange Office (FXO) - a service that can be ordered from the telephone company that provides local telephone service from a central office that is outside (foreign to) the subscriber's exchange area. To generate a call from the computer telephony system to the POTS set, you will need a FXS connection configured. See also FXS.

Foreign Exchange Station (FXS) - Interface that connects directly to a standard telephone, fax machine, or similar device over a standard RJ-11 modular telephone cable, and supplies ringing voltage, dial tone, and similar signals to it. see FXO

Framing - A procedure for controlling errors. Consists of inserting bits so the receiver can identify the time slots allocated to each subchannel

G

Gatekeeper - is the central control entity that performs management functions in a Voice and Fax over IP network and for multimedia applications such as video conferencing. Gatekeepers provide intelligence for the network, including address resolution, authorization, and authentication services, the logging of call detail records, and communications with network management systems. Gatekeepers also monitor the network for engineering purposes as well as real-time network management and load balancing, controlling bandwidth, and providing interfaces to existing legacy systems.

Gateway - an entrance into and out from a communications network. Technically, a gateway is an electronic repeater that intercepts and steers electrical signals from one network to another.

Greeting - voice messages that are played to the Quadro users or users calling to the Quadro activating specific services.

H

Hold Music - music played to the party that is on hold.

Host - an intelligent device attached to the network; can be also a mainframe computer.

Host Name - the name given to a mainframe computer or device.

Hunt Grouping - the Quadro service that allows configuring several users over Quadro to ring in series when a specific call arrives.

Hypertext Transfer Protocol (HTTP) - the protocol used by Web browsers and Web servers to transfer files, such as text and graphics files.

I

Integrated Services Digital Network (ISDN) - is a system of digital phone connections which allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. There are two basic types of ISDN service: Basic Rate Interface (BRI) and

Primary Rate Interface (PRI). BRI is a basic service is intended to meet the needs of most individual users. PRI is intended for users with greater capacity requirements

Internet Control Message Protocol (ICMP) - a network-layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

Internet Protocol (IP) - a unique, 32-bit number for a specific TCP/IP host on the Internet, normally printed in decimal form (for example, 128.122.40.227). Part of the TCP/IP family of protocols, it describes the software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages.

Internet Service Provider (ISP) - a vendor who provides direct access to the Internet or a company that provides Internet access to other companies and individuals.

Intrusion Detection System (IDS) - is a firewall, but together with deleting the dangerous packets or packets including intrusion attacks, IDS also keeps information about dropped packets and the senders responsible for them.

IP address - also known as the Internet Address, is a unique 32-bit identifier for a specific TCP/IP host computer on a network. IP addresses are in dotted decimal form, such as 192.168.10.26, with each of the four address fields assigned as many as 255 values.

IP address Mask - A range of IP addresses defined so that only machines with IP addresses within the range are allowed access to an internet service. To mask a portion of the IP address, replace it with the asterisk wild card character (*). For example, 192.44.*.* represents every computer on the internet with an IP address beginning with 192.44

IP Gatekeeper - defines the policies that govern a multimedia system such as dialing plans, user privileges, bandwidth consumption, and others. The gatekeeper also provides the means to extract information from such a system for various purposes, e.g., billing information, users that are logged in, etc. The gatekeeper is also a focal point for the introduction of supplementary services.

IP Gateway - most commonly, a network device that converts voice and fax calls, in real time, between the public switched telephone network (PSTN) and an IP network. The main IP gateway functions include voice, fax, compression/decompression, packetization, call routing, and control signaling. Additional features may include interfaces to external controllers, such as gatekeepers or soft-switches, billing systems, and network management systems.

IP PBX - an enterprise-based IP data network device that switches VoIP telephone traffic.

IP Telephony - a technology that allows voice phone calls to be made over the Internet or other packet networks using a PC via gateways and standard telephones.

IPSec - is used to provide security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers.

J

Jitter Buffer - the buffer that collects incoming packets to place them in the right order. If the network has a high delay variation, increasing the Jitter Buffer can improve the audio quality, but this also increases the delay.

L

LED - Light-Emitting Diode, A semiconductor device that emits visible light when conducting current. Has replaced incandescent lamps as indicators in most electronic equipment.

Lifeline POTS - a voice telephone line that works even if electricity is cut off at the customer premises, since the line is powered from emergency backup at the central office. Multiple lifeline POTS lines can be delivered on one copper pair with the use of a digital line powered pair gain system. A basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

Local Area Network (LAN) - a short distance data communications network (typically within a building or campus) used to link computers and peripheral devices under some form of standard control.

Login -the procedure of identifying a user with a username and a password to enter into the protected field.

M

Many Extensions Ringing - a Quadro service that allows configuring several users over Quadro to ring simultaneously when a specific call arrives.

Media Access Control (MAC) Address - the address for a device as it is identified at the Media Access Control layer in the network architecture.

Media Access Control (MAC) Layer - is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

Media Gateway - a generic class of products grouped under the Media Gateway Control Protocol (MGCP). A major function of the media gateway is simple IP/TDM conversion under the control of a softswitch.

N

Name server - a directory service that provides a mapping between a resource's global name and its physical location in the network.

Network Address Translation (NAT) - is used to allow LAN devices that do not have their own static IP addresses to connect to the Internet sharing an IP address. NAT will assume control of assigning their IP address. Furthermore, the NAT takes care that packets will reach the LAN PC that originated the traffic. This mechanism is absolutely transparent for the users (or the PCs in the LAN).

Network Time Protocol (NTP) - a protocol that is used for time counting in the Internet, based on the atomic clocks with the precision in milliseconds. This is the recommended protocol for synchronizing the time of hosts in the network.

P

Packetization Interval - the time interval between two RTP packets of the same stream. If the interval is increased, the overhead is decreased but the voice quality might deteriorate. If the interval is decreased, the network load is increased and the delay is reduced.

Password - a secret alphanumeric string used to identify and to allow the user to have access to a system.

PCM - a form of modulation in which the information signals are sampled at regular intervals and a series of pulses in coded form are transmitted representing the amplitude of the information signal at that time.

Point-to-Point Protocol (PPP) - allows a computer to connect to the Internet with a standard dial-up telephone line and a high-speed modem and to enjoy most of the benefits of the direct connection.

Point-to-Point Tunneling Protocol (PPTP) - enables virtual private networking - enabling secure remote access to corporate networks over the Internet.

POTS (Plain Old Telephone Service) - is the standard telephone service that most homes use. It is also referred to as the PSTN, or the Public Switched Telephone Network

Private Branch Exchange (PBX) - a telephone switch owned privately, usually by a large company. If it owns a PBX, a company does not need to lease a telephone line for each telephone set at a site.

Proxy server - an intermediate device that receives SIP requests from a client and then initiates requests on the client's behalf.

Public Switched Telephone Network (PSTN) - refers to the local telephone company.

R

Real-Time Transport Protocol (RTP) - the Internet-standard protocol for the transport of real-time data, including audio and video, allows applications to synchronize audio and video information. RTP connections are established between servers across the Internet after voice has been converted to IP format. RTP is used in virtually all Voice-over-IP architectures, for videoconferencing, media-on-demand, and other applications.

Real-Time Transport Control Protocol (RTCP) - is the control protocol that works in conjunction with RTP. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants. Feedback of information to the application can be used to control performance and for diagnostic purposes.

Registration - procedure of user subscribing to a server. Usually some personal parameters such as username, password, etc., are required upon registration.

Remote Testing - remote connection from the Epygi Support office to the customer's Quadro for testing and/or for troubleshooting.

Router - A device that determines the next network point to which a data packet should be forwarded enroute toward its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet

RSA - is an asymmetric key system. It must be available on both sides of the VPN and generates on each side a different pair of keys, a private and a public key.

S

Security Parameter Index (SPI) - is an index to keep VPN tunnels distinct. A security association is defined by destination, protocol and SPI. Without the SPI, connections to the same gateway using the same protocol would not be distinguishable.

Session Initiation Protocol (SIP) - is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. SIP is increasingly used for Internet telephony signaling, in gateways, PC phones, softswitches, and softphones, but it is not limited to Internet telephony, and can be used to initiate and manage any type of session, including video, interactive games, and text chat.

Signaling - a process of sending a transmission signal over a physical medium for communication.

Silence Suppression - a method that allows disabling RTP packet transmission when there is no voice activity. This feature helps to avoid extra traffic when the RTP stream doesn't contains voice data.

Simple Network Management Protocol (SNMP) - the Internet standard protocol developed to manage nodes on an IP network.

SIP address - unique address of the users registered on the SIP server. The address can be used to connect the user. The full SIP address has the following format: "display name" <username@ipaddress:port>.

SIP server - this server is used for registering users. It gives a possibility to make IP connections between users registered on the same SIP server.

Software - PC programs.

Software PBX - a telephone system that converges voice and data on an industry-standard computing platform and uses computer telephony components that conform to industry standards. Since they conform to industry standards, software PBXs are interoperable with third-party systems and CT components. Conformance also allows software PBXs to run third-party enhanced applications such as desktop call control, graphical voice mail, automatic call distribution (ACD), IP gateways, follow-me call forwarding, unified messaging, and CRM integration.

Speed Calling - a service that allows making a personal address book for every Quadro user. A simple digit combination can be assigned to any destination phone number.

T

Transfer - a service giving a possibility to readdress incoming calls. Call Transfer can be conditional (with consultation) and unconditional (without consultation).

Transmission Control Protocol (TCP) - a connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Transmission Control Protocol/Internet Protocol (TCP/IP) - is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

Trunk - is a communications channel between two points, typically referring to large-bandwidth telephone channels between switching centers that handle many simultaneous voice and data signals.

Trunk Level 1 (T1) - a high-speed (1.544Mb/s) digital telephone line with the equivalent of 24 individual 64Kb/s channels that are joined via time division multiplexing. A T1 line can be used to transmit voice or data, and many are used to provide connections to the Internet. T1 is the North American equivalent of an E1 line.

U

UDP - a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagram without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.

Universal Serial Bus (USB) - is an interface with a protocol that is designed to handle a broad range of devices - telephones, modems, printers, etc.

Upstream- in communications, there are two circuits - one coming toward you and the other going away from you. Upstream is another term for the name of the channel going away from you.

URL - an identifier used to locate content that is transported via the HTTP protocol.

Username - identification name of the user. Usually used for registration and login.

V

VCI - parameter used to configure ATM settings and is usually given by the Internet provider.

Virtual Private Network (VPN) - connects two local networks (intranets) over the insecure Internet securely. VPN routers manage authentication between servers and clients and handle data encryption for the connection. Only authorized users can access the network and the data exchange cannot be intercepted. A VPN includes authentication and encryption to protect data integrity and confidentiality. VPNs are "virtual" in the sense that individuals can use the public Internet as a means of securely accessing an internal network. Once the VPN connection is established, users have access to the same network resources, addresses, and so forth as if they were connected locally. VPNs are "private" because the data is encrypted between two VPN gateways. Encryption makes it very difficult for anyone to intercept data and capture sensitive information such as passwords.

Voice mail - a brief message that external users can leave for the Quadro users in the event that nobody answers the call.

Voice Mail System (VMS) - a feature providing the possibility of leaving brief voice messages at the unavailable or busy Quadro extension's mailbox.

Voice mailbox - is the mailbox where voice mails are collected.

Voice message - help messages that are played to the user giving a hint on how to manipulate the menus within Quadro using the phone handset.

Voice Over Internet Protocol (VOIP) - technology used to transmit voice conversations over a data network using the Internet Protocol. The ability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality.

VPI - parameter used to configure ATM settings usually given by the Internet provider.

W

Wide Area Network (WAN) - a communications network used to connect computers and other devices across a large area.

Windows Internet Naming Service (WINS) - a database with all PC hostnames and IP addresses connected to them in the TCP/IP environment.

Appendix: Software License Agreement

EPYGI TECHNOLOGIES, LTD. Software License Agreement

THIS IS A CONTRACT.
CAREFULLY READ ALL THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. USE OF THE QUADRO HARDWARE AND OPERATIONAL SOFTWARE PROGRAM INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE HARDWARE OR SOFTWARE.

- License.** Epygi Technologies, Ltd. (the "Licensor"), hereby grants to you a non-exclusive right to use the Quadro Operational Software program, the documentation for the software and such revisions for the software and documentation as the Licensor may make available to you from time to time (collectively, the "Licensed Materials"). You may use the Licensed Materials only in connection with your operation of your Quadro. You may not use, copy, modify or transfer the Licensed Materials, in whole or in part, except as expressly provided for by this Agreement.
- Ownership.** By paying the purchase price for the Licensed Materials, you are entitled to use the Licensed Materials according to the terms of this Agreement. The Licensor, however, retains sole and exclusive title to, and ownership of, the Licensed Materials, regardless of the form or media in or on which the original Licensed Materials and other copies may exist. You acknowledge that the Licensed Materials are not your property and understand that any and all use and/or the transfer of the Licensed Materials is subject to the terms of this Agreement.
- Term.** This license is effective until terminated. This license will terminate if you fail to comply with any terms or conditions of this Agreement or you transfer possession of the Licensed Materials to a third party in violation of this Agreement. You agree that upon such termination, you will return the Licensed Materials to the Licensor, at its request.
- No Unauthorized Copying or Modification.** The Licensed Materials are copyrighted and contain proprietary information and trade secrets of the Licensor. Unauthorized copying, modification or reproduction of the Licensed Materials is expressly forbidden. Further, you may not reverse engineer, decompile, disassemble or electronically transfer the Licensed Materials, or translate the Licensed Materials into another language under penalty of law.
- Transfer.** You may sell your license rights in the Licensed Materials to another party that also acquires your Quadro-4x or any Quadro SIP Gateway product. If you sell your license rights in the Licensed Materials you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.
- Protection And Security.** Except as permitted under Section 5 of this Agreement, you agree not to deliver or otherwise make available the Licensed Materials or any part thereof to any person other than the Licensor or its employees, without the prior written consent of the Licensor. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution thereof, in whole or in part, in any form, shall be made.
- Limited Warranty.** The only warranty the Licensor makes to you in connection with this license is that the media on which the Licensed Materials are recorded will be free from defects in materials and workmanship under normal use for a period of one (1) year from the date of purchase (the "Warranty Period"). If you determine within the Warranty Period that the media on which the Licensed Materials are recorded are defective, the Licensor will replace the media without charge, as long as the original media are returned to the Licensor, with satisfactory proof of purchase and date of purchase, within the Warranty Period. This warranty is limited to you as the licensee and is not transferable. The foregoing warranty does not extend to any Licensed Materials that have been damaged as a result of accident, misuse or abuse.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE LICENSED MATERIALS ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT AS DESCRIBED ABOVE, THE LICENSOR MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE LICENSED MATERIALS ARE, OR WILL BE, FREE FROM ERRORS, DEFECTS, OMISSIONS, INACCURACIES, FAILURES, DELAYS OR INTERRUPTIONS INCLUDING, WITHOUT LIMITATION, TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES AND ACCURACY OR COMPLETENESS OF RESPONSES, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE LICENSED MATERIALS REMAINS WITH YOU.

- LIMITATION OF LIABILITY AND REMEDIES.** IN NO EVENT SHALL THE LICENSOR OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS, ARISING OUT OF THE USE OF OR INABILITY TO USE THE LICENSED MATERIALS, EVEN IF THE LICENSOR OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU AGREE THAT YOUR EXCLUSIVE REMEDIES, AND THE LICENSOR'S OR SUCH OTHER PARTY'S ENTIRE LIABILITY WITH RESPECT TO THE LICENSED MATERIALS, SHALL BE AS SET FORTH HEREIN, AND IN NO EVENT SHALL THE LICENSOR'S OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU EXCEED THE LICENSE FEE PAID FOR THE LICENSE MATERIALS.

The foregoing limitation, exclusion and disclaimers apply to the maximum extent permitted by applicable law.

9. **Compliance With Laws.** You may not use the Licensed Materials for any illegal purpose or in any manner that violates applicable domestic or foreign law. You are responsible for compliance with all domestic and foreign laws governing Voice over Internet Protocol (VoIP) calls.
10. **U.S. Government Restricted Rights.** The Licensed Materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights clause at 48 C.F.R. section 52.227-19, or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227.7013, as applicable.
11. **Entire Agreement.** It is understood that this Agreement, along with the Quadro Installation Guide and User's Manual, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.
12. **No Waiver.** Failure by either you or the Licensor to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way be considered to be a waiver of such provisions or rights, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid or unenforceable in any respect, the validity and enforceability of the remaining provisions shall not be affected.
13. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the state of Texas, without regard to choice of law provisions that would cause the application of the law of another jurisdiction.
14. **Attorneys' Fees.** In the event of any litigation or other dispute arising as a result of or by reason of this Agreement, the prevailing party in any such litigation or other dispute shall be entitled to, in addition to any other damages assessed, its reasonable attorneys' fees, and all other costs and expenses incurred in connection with settling or resolving such dispute.

If you have any questions about this Agreement, please write to Epygi at 6900 North Dallas Parkway, Suite 850, Plano, Texas 75024 or call Epygi at (972) 692-1166.