InterChange iQ 2030 Series Gateway User Guide

WESTELL

Notice

Trademarks

Change History

Issue	Product	Status	Date
001	IiQ2030 Gateway User Guide	First Issue	May 2002
		Rev. 01	Jun 2002
		Rev. 02	Jul 2002
		Frozen	Aug 2002
002	IiQ2030 Gateway User Guide	Rev. 03	Oct 2002
		Frozen	Jan 2003
003	IiQ2030 Gateway User Guide	Rev. 04	Feb 2003
004	Release 1.4 of IPH-DP Appln.	Rev. 05	Mar 2003
005	Release 1.5 of IPH-DP Appln.	Rev 06	Jun 2003
006	Release 1.6 of IPH-DP Appln.	Rev 07	Mar 2004

Copies of this User Guide are available in other languages at additional cost on request from:

Westell Limited
Ringway House, Bell Road
Daneshill
Basingstoke
Hampshire, RG24 8FB
United Kingdom

Tel: +44 (0) 1256 843311
Fax: +44 (0) 1256 840429
Help Line: +44 (0) 1256 842285
email: info@westell.co.uk
Website: www.westell.co.uk

Document number: UM 400 01 010

Contents

1 Introduction

1.1 Scope of this Guide

This Guide is intended for trained personnel familiar with SCN and IP protocols and their network topology. It describes the hardware configuration and management of the InterChange iQ 2030 Series Gateway product, its installation, maintenance and general operation. Throughout this document it will be referred to as the IiQ Gateway.

The Guide is divided into the following sections:

1 Introduction.

2 Installation

3 Initial Configuration

4 Management

5 Diagnostics

6 Transparent Signalling

7 SCN Clock Synchronisation

8 SNMP Traps

9 Craft Port Management

10 Fault Determination

Appendices

A Safety Instructions

B References & Technical Specifications

C Connectors & Cabling

D Glossary of Terms

E Useful Information

1.2 Management

Management of the IiQ Gateway is divided between its signalling functions and media functions.

Basic configuration is achieved using a PC running Hyperterminal (or similar application) connected to the Craft port using the serial cable supplied with the IiQ Gateway.

Once the basic configuration is complete, full configuration and management of the unit is achieved using a Web browser on a networked PC.

Factory default settings were installed during manufacturing. For any advanced engineering support under the guidance of a Westell support engineer, an additional cable will be required (details may be found in *Appendix C - Craft Port - Factory Mode*).

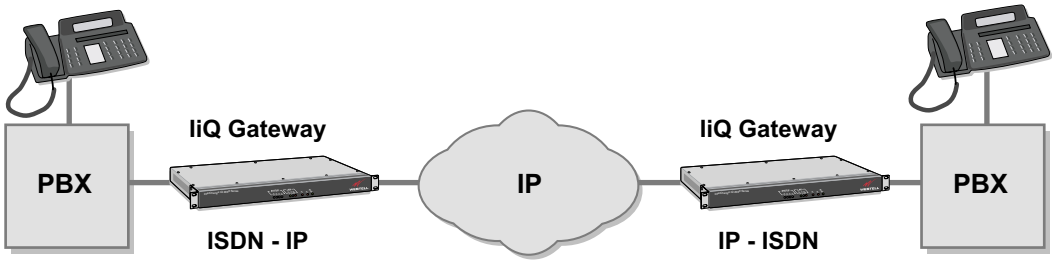
1.3 Product Overview

The IiQ Gateway is a combined signalling and media unit used to connect an existing circuit switched PBX to an IP network allowing voice and fax calls to be passed across the IP network instead of using more expensive ISDN lines. The IiQ Gateway provides the following functionality:

- Conversion between circuit switched DPNSS signalling and H.323 IP signalling.
- Tunnel DPNSS signalling through a H.323 IP network.
- Conversion between circuit switched Bearer channels and IP packets.
- Call routing.
- Support for voice and fax calls.
- Transfer of DTMF tones across an IP network.

PBX to IP Calls.

The IiQ Gateway allows calls to be made between the PBX and IP networks as shown in the figure above and also offers PBX transparency over IP, as shown in the figure below.



PBX Transparency over IP.

Call routing is achieved either by using internal routing tables or by using external Gatekeeper services. See example system configurations in *Section 3.5*.

The basic installation of the IiQ Gateway should take no more than thirty minutes and includes the setting up of the IP addresses, building an external pre-defined routing database and simple DPNSS configuration.

A fully configured IiQ Gateway with two Ports is capable of supporting up to 60 concurrent voice calls (depending on model) using any combination of voice codecs. However, the number of channels available will depend on the unit model and Channel Licences purchased.

1.4 The Product Series

1.4.1 Product Variants

Variations available in the IiQ 2030 Series of Gateway products provide a range of channels depending on the DSP installed and Channel Licences purchased.

InterChange Model	No. of Ports	No. of Channels
iQ 2031EL	1	15 or 24
iQ 2031	1	Fixed at 30
iQ 2032	2	30 or 60

The IiQ 2031EL is the entry level unit and can be supplied with a licence for 15 or 24 channels. The unit will have been pre-configured for the channels licensed with order.

The IiQ 2031 is the Gateway unit with a 30 channel licence. The unit will have been pre-configured. This unit cannot be upgraded.

The IiQ 2032 is supplied with a minimum of a 30 channel licence and will have been pre-configured with this and any other licence purchased with order.

1.4.2 Channel Licence Upgrades

Apart from the IiQ 2031 Gateway, the number of configurable channels may be upgraded by purchasing an additional licence to the maximum permitted for the gateway unit supplied. Please contact your supplier for details.

Note: Once a channel licence has been allocated to a specific gateway unit, it cannot be reallocated or transferred to another unit unless the IiQ Gateway is returned to the factory.

2 Installation

Before you can use your IiQ Gateway, you will need to follow all of the steps in this section. This will provide you with basic functionality. Configuration of the more advanced features of the IiQ Gateway are described in section *3 Initial Configuration* and section *4 Management*.

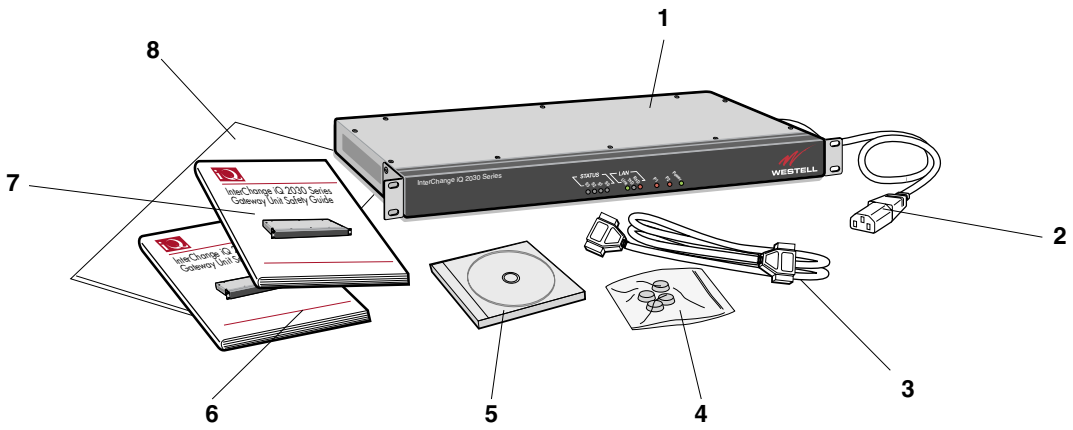
Important:

Before unpacking the unit, please check that you have received the product and licensed channels ordered. The package carton label will show:

- Stock Number
- Product Description
- Serial Number
- Software Version
- Total Number of Channels Available

Contact the supplier if there is any discrepancy.

2.1 Unpacking & Inspection



The Package Contents

The IiQ Gateway is supplied in a single package containing the following:

1 IiQ Gateway Unit

2 Mains Power Cable

3 Serial Cable for Craft Port (Craft Mode)

4 Pack of 4 feet (for desktop mounting)

5 CD-ROM with PDF versions of User Documentation

6 Quick Start Guide

7 Safety Guide.

All other cables are to be supplied by the customer. Please refer to *Appendix C Connectors & Cabling* for details.

Store the packaging material in a clean, dry area for possible re-use.

2.2 Hardware Installation

The IiQ Gateway may be either rack mounted (preferred) or used as a desk top unit. When used as a desk top unit, four plastic feet are supplied and should be affixed on the base at each corner.

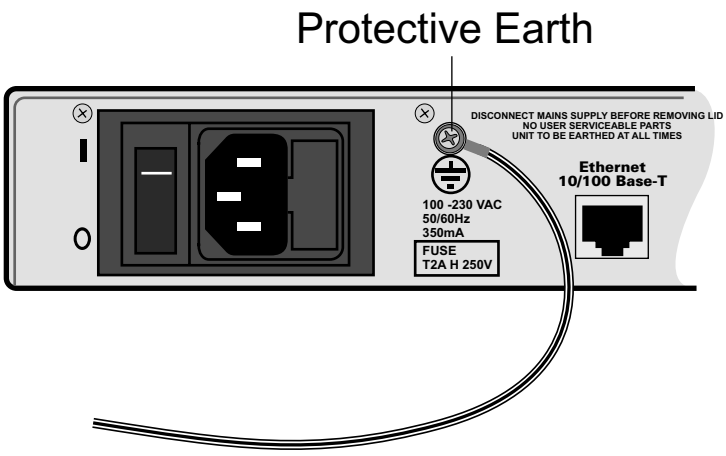
When rack mounting, attention should be paid to cooling. As the IiQ Gateway has side to side cooling the design of the rack should allow for adequate airflow either side of the unit. Refer to the rack manufacturer's specification for suitable mounting methods.

Caution:

The IiQ Gateway must be earthed at all times via the protective earth terminal on the rear of the unit.

The earthing cable must conform to the following specification. It shall:

- be PVC covered green with yellow longitudinal coloured stripes as defined in EN 60950,
- be rated at 17 amps,
- have a cross sectional area of 1.5 m^{m2},
- be of stranded wire 7/0.53, and
- be terminated with an M3 ring terminal 1-2.6 mm^2 conductor.



View showing earth screw on rear panel.

2.2.1 Connection Sequence

To identify the ports, please refer to the illustration in section 2.4.

1 Connect the protective safety earth as described above.

2 Connect the mains power cable.

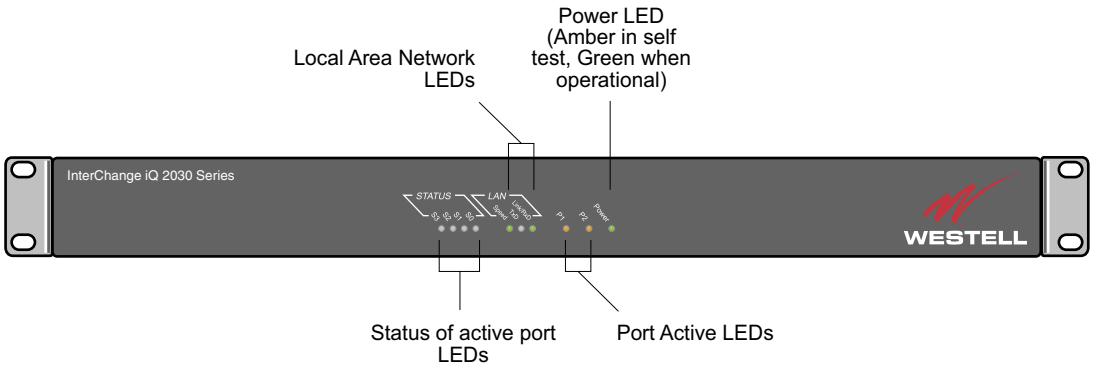
3 Connect the serial cable to the Craft Port.

4 Connect the 10/100 Ethernet cable.

Note: The Ethernet connection should now be regarded as permanent.

Do not connect to the E1 telephony ports or the Ethernet cable to the IP Network until first time configuration is complete and the IP Addresses are set up.

2.3 The IiQ Gateway Unit



Front view of an IiQ Gateway unit.

2.3.1 LEDs

The IiQ Gateway unit has 10 LEDs on its front panel. They show unit status information.

STATUS

There are 4 red Status LEDs; S3, S2, S1 and S0. They indicate unit status in conjunction with the two port LEDs, P1 and P2. During unit self-test, the status LEDs will come on and go off in sequence, and in the event of a self-test failure, stop with one LED remaining on.

LAN

Three LEDs indicate LAN activity. The TxD LED flashes AMBER on transmission of a packet. The Link/RxD LED flashes GREEN on receipt of a packet. The GREEN Speed LED is ON for 100 Mbs or OFF for 10Mbs. If Ethernet is not connected, these LEDs will be off.

Note: The RxD LED will flash for any traffic on the Ethernet, regardless of destination.

P1 & P2

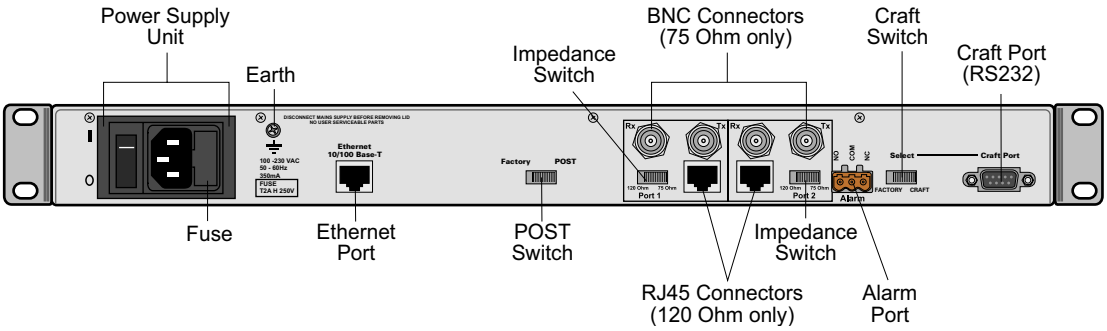
There are two AMBER Port LEDs, P1 and P2. Together with the Status LEDs, they indicate unit status. When the unit is operating correctly, these LEDs ripple, with all status LEDs off.

When a problem exists, the Port LEDs will show its location (P1 or P2, or if both P1 and P2 are lit, a major alarm exists). The status LEDs will then indicate the problem. If more than one has a problem, they will be shown in a cycle of five seconds each.

Power

The Power LED has two functions. When power is applied, it comes on amber to indicate the unit is in self-test mode. When the self-test has been satisfactorily completed, it changes to green to indicate the unit is functioning correctly.

2.4 Back Panel Equipment



Rear view of an IiQ2030 Series Gateway unit.

2.4.1 Ports

Ethernet Port

The 10/100 Base-T Port is used to connect to the IP Network to allow voice packets to be transmitted and received and for a PC using a Web browser to communicate with the IiQ Gateway's configuration and management interface.

Port 1 & Port 2

Each port has three connectors. The two BNC connectors are 75Ω unbalanced and are marked Rx and Tx. The RJ45 connector is 120Ω balanced. The Impedance Switch must be set to the correct impedance. Parameters for each port are configurable using a Web browser.

Craft Port

The Craft Port is provided primarily to enable a serial connection to a dumb terminal or a terminal emulation application on a PC running RS-232 at 9600baud, 8 bit, 1 stop bit and no parity. A cable is supplied for this connection.

It is also used for Factory Engineering management but must only be used under supervision of a Westell Engineer and will require a different cable. Details for this cable can be found in *Connectors & Cabling - Craft Port - Factory Mode.*

Alarm Port

If required, you can connect the IiQ Gateway's Alarm Port to an alarm signal detector before powering on the unit.

2.4.2 Switches

Power On/Off

The power On/Off switch is adjacent to the mains connector. Before connecting any cables (other than the E1 cables) or changing any switches, power off the IiQ Gateway unit.

POST switch

The Power On Self Test switch must be set in the **POST** position before powering on the IiQ Gateway unit. The Factory position is for Westell Engineers only.

Impedance Switch

This allows the selection of either 75Ω or 120Ω impedance for the SCN ports. 75Ω should be used for co-axial BNC connection and 120Ω for UTP RJ45 connectivity. Selection must be made before power is applied to the unit.

Craft Switch

Used to switch between serial connection for initialising the IiQ Gateway and Factory Engineering management. By default the switch should be set to **CRAFT**.

2.5 Power On Self Test and IP Address Set Up

When an IiQ Gateway is powered on for the first time it must have its IP addresses and sub-net masks configured as part of self-test.

1 Before powering on the unit, establish a serial connection between the **Craft Port** and a dumb terminal or a terminal emulation application on a PC running RS-232 at 9600 baud, 8 bit, 1 stop bit, no parity.

2 Power **ON** the IiQ Gateway unit.

The unit will perform half of the power on self-test sequence. The **Power** LED on the front panel shows AMBER and the four **STATUS** LEDs come on and go off (in sequence from left to right) to indicate the unit is performing the self-test. These tests check the correct operation of the hardware functions. The unit will then require IP addresses and sub-net masks. When requested:

3 Enter the **Management IP address**.

4 Enter the **Management Sub Net Mask**.

5 Enter the **Management Default Gateway**.

6 Enter the **Media IP address**.

7 Enter the **Media Sub Net Mask**.

8 Enter the **Media Default Gateway**.

The self-test will then run to completion, which is indicated by the terminal displaying the management **IP address** and **Sub Net Mask** required to access the IiQ Gateway unit on an IP network.

9 Power cycle the IiQ Gateway. This time the power on self-test will run to completion without user intervention and should complete in less than one minute.

10 On completion of a successful self-test, remove the serial connection. Failure to do so may result in the IiQ Gateway not restarting.

Successful Self-Test

When all the tests have completed successfully, the Self-Test module invokes the Loader module. The **Power** LED changes colour from AMBER to GREEN.

Note:

If only one E1 Port is in use (as with the IiQ 2031), then the LEDs for the unused port will show red. This is not a fault condition.

Self-Test Failure

If any test in the sequence fails then the cycle of the **STATUS** LEDs will stop (with one LED remaining on) and the **Power** LED will remain AMBER.

Details of any failures may be obtained if the unit undergoes the self-test when connected via the Craft Port to a dumb terminal or a terminal emulation application on a PC running RS-232 at 9600 baud, 8 bit, 1 stop bit and no parity.

If an error is reported, consult the Fault Determination section for the appropriate corrective action. Once errors have been corrected make sure the self-test runs satisfactorily to completion.

If no failures have occurred during the self-test, the self-test software passes control on to the operational software.

Only proceed when the unit passes the self test sequence.

Note:

Do NOT configure any further parameters using the Terminal Emulation programme. The remaining configuration changes are made via the Gateway Management Interface and are described in the next section.

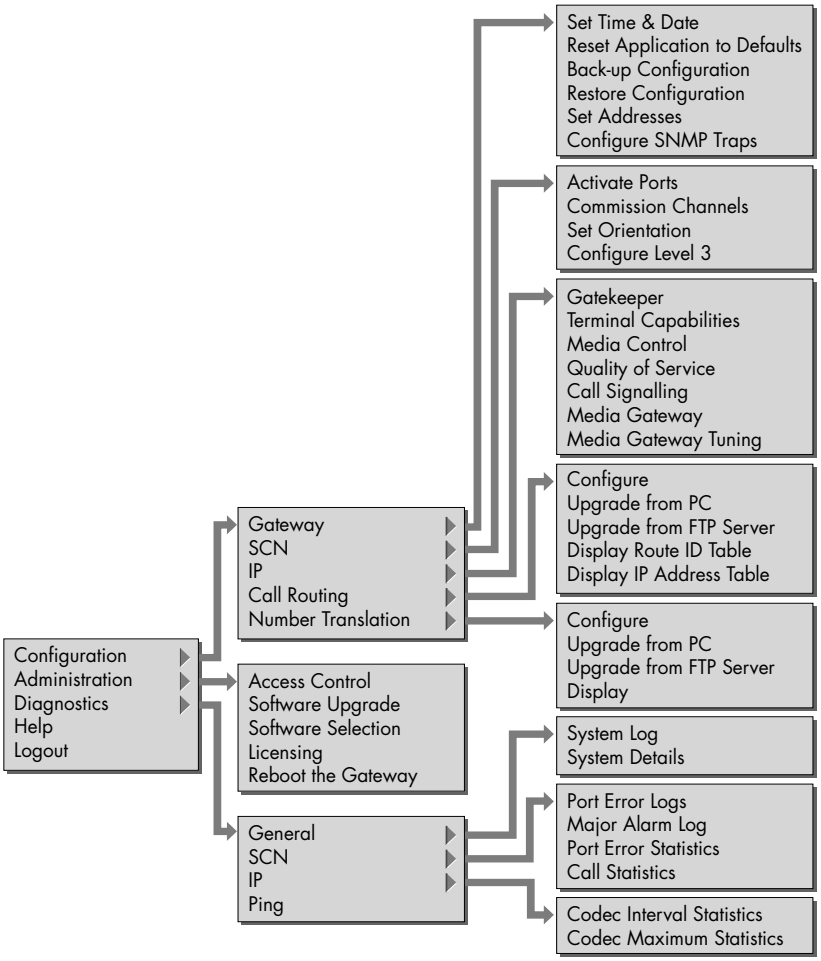
3 Initial Configuration

3.1 Gateway Management Interface

To configure the IiQ Gateway, you must now connect the Ethernet Port to the IP Network, but do NOT connect to the E1 telephony ports yet.

A standard Web browser application is required to configure the IiQ Gateway unit. Internet Explorer v. 5.0 or later or Netscape v. 6.0 or later are recommended. Ensure your browser is set to accept cookies and always check for newer versions of stored pages.

Configuration parameters are set using a simple intuitive menu as shown below:



Configuration Menu Structure.

Buttons on many pages have the same function:

Submit	Use this to submit the configuration setting or change.
Refresh	Use this to refresh the page to see the original settings or to confirm the submitted settings or changes.
Close	This takes you back to the Menu or previous pages.

3.2 Access Levels

There are three Access levels:

- Monitor
- Configure
- Advanced

Monitor allows the User to see details of the current configuration and diagnostics but disallows changes.

Configure allows the User to configure all except the following parameters:

- Set to Defaults
- Access Control
- Restore Configuration
- Software Upgrade
- Software Selection
- Licensing
- Engineering Settings

Advanced allows the User to reboot the IiQ Gateway and change all parameters including those disallowed above.

3.3 Help Facility

This is available from the Main menu and will open a separate browser window which may be kept open at the same time as the Configuration window. However, it does not have the level of detail of this User Guide and does not provide guidance on communications protocols.

3.4 Logout

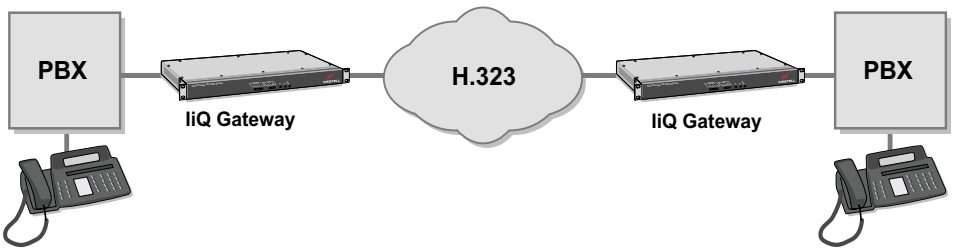
The Logout facility is provided as only a single user may access the IiQ Gateway's management interface at any one time. When a user is logged in, no other logins will be accepted and you should **Logout** at the end of the session.

An inactivity timer is provided if a user does not logout. This will enable another user to log in after a set period of non activity in the event of a network or PC failure. The factory default value for the Non-Use Timeout Period is 5 minutes but it may be set from between 3 and 15 minutes. When the Non-Use Timeout Period expires, it does not log the user out; this does not occur until another user attempts to log in.

Note: When using Internet Explorer, if you close the browser or navigate to another location without first logging out, a window will pop up to ask if you want to log out from the Gateway Management Interface. Selecting **Logout** will enable another user to login immediately. Selecting **Ignore** will close the window and leave you logged in until the Non-Use timeout period has elapsed.

3.5 Configuration Examples

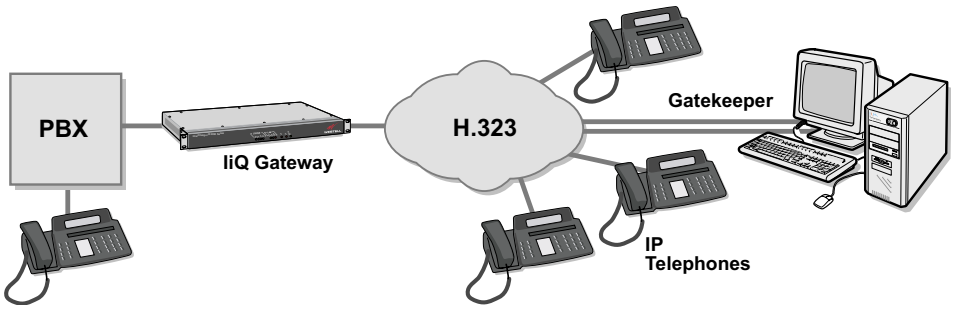
3.5.1 Using Internal Routing



PBX to H.323 Device using Internal Routing.

When the IiQ Gateway is configured for internal Routing, both a Route ID Table and an IP Address Table are required.

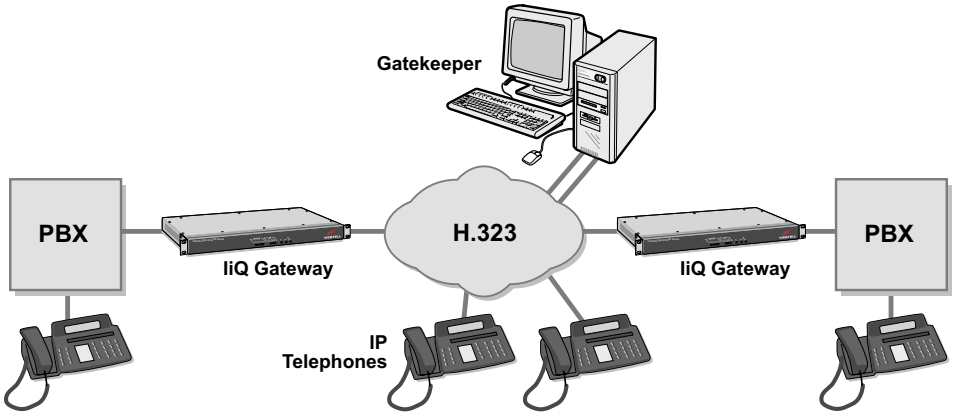
3.5.2 Using a Gatekeeper or IP Telephony Server



PBX to H.323 Device using a Gatekeeper or an IP Telephony Server.

When the IiQ Gateway is configured for routing through a Gatekeeper or an IP Telephony Server, a Route ID Table and an IP address Table are not required.

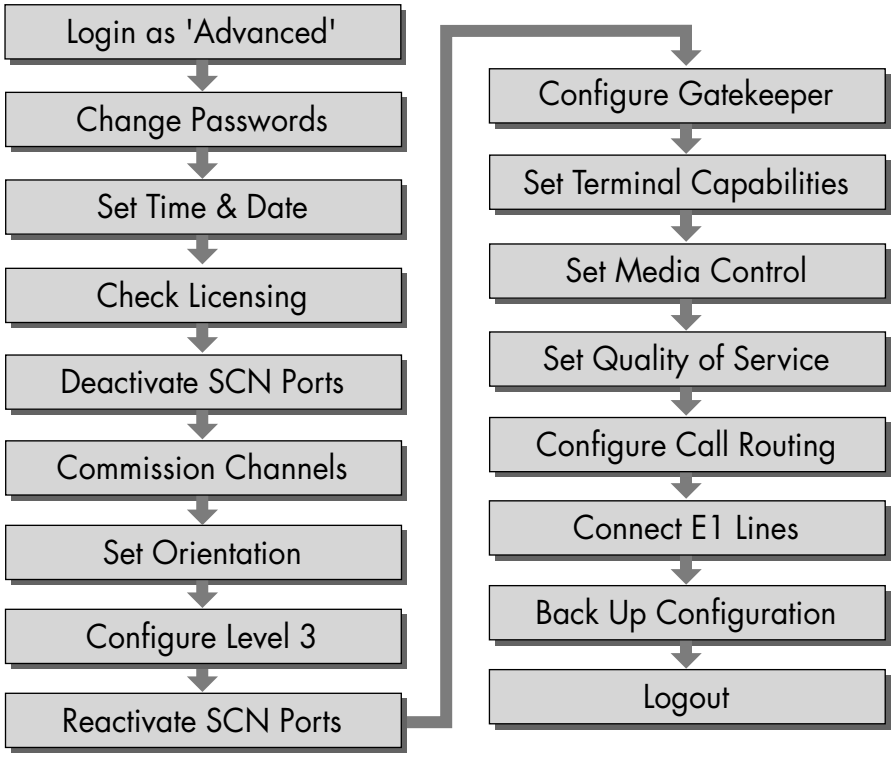
3.5.3 Using a Gatekeeper or IP Telephony Server with Internal Routing



PBX to H.323 using a Gatekeeper or an IP Telephony Server with Internal Routing

When the IiQ Gateway is configured for Internal Routing with a Gatekeeper or an IP Telephony Server, only a Route ID Table is required.

3.6 First Time Software Configuration.



First Time Software Configuration Process.

3.6.1 Name & Password Defaults

The factory default settings for the Name or User ID and Password are the same as for the levels of access. For example, to access the interface at Monitor level, the Name is **Monitor** and the Password is also **Monitor**. Name or User ID is always the level of Access. Only the password may be changed. Name or User ID and passwords are case sensitive.

We recommend that you change the default passwords. This can only be carried out at the Advanced level.

3.6.2 Application Default Settings

At any time during the configuration process you can undo your settings and start again by resetting the IiQ Gateway to its default settings. Refer to section *3.7 Resetting Applications to Default.*

3.6.3 Login

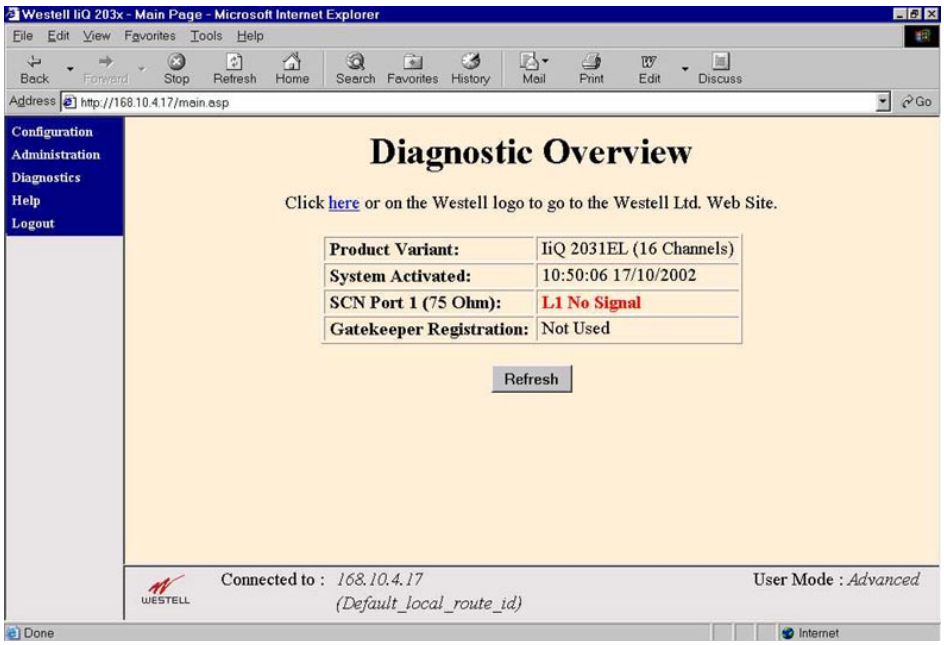
To access the Gateway Management Interface:

1 Type in the Management IP address of the IiQ Gateway in the Address field of your browser. When the IiQ Gateway unit is located, you will be asked to enter a Name or User ID and a Password.

2 For Name or User ID type in **Advanced**.

3 For Password type in **Advanced**. An introduction screen will appear.

4 Click on **Continue** and the top level Menu will appear.



The Top Level Menu and Diagnostic Overview Screen.

The Diagnostic Overview screen shown is that of the IiQ 2031 gateway unit. The IiQ 2032 screen is similar but also shows SCN Port 2.

3.6.4 Change Passwords

Note: Passwords are case sensitive.

1 Select **Administration** and then **Access Control**.

2 Select the **Access level** field and type in the new password.

3 Select the next field and retype in the new password.

The operation is the same for other access levels.

4 Select **Submit** and the **Change Confirmation** screen will appear.

5 Select **Go Back** to return to **Access Control Settings**.

6 Select **Close** to exit **Access Control**.

Note: Once the password has been changed, you will not be able to change any parameters until you logout and login again with the new Password.

7 Logout and then log in again with the new password at either the *Advanced* or the *Configure* level.

3.6.5 Set Time & Date

1 Select **Configuration**, **Gateway** and then **Set Time & Date**.

2 Select **Synchronise with PC** (if the PC clock is set correctly), or key in the correct values and then **Set with current values**.

3 Select **Close** to return to the Menu.

3.6.6 Check Licensing

The Diagnostic Overview screen will indicate the product variant (IiQ 2031EL, IiQ 2031, IiQ 2032, etc.) and the number of licensed channels in the **Product Variant:** field. Units will have been pre-configured before leaving the factory to enable the number of channels stated at the time of order. Before proceeding, this should be checked and corrected if necessary.

1 Select **Administration** and then **Licensing**.

2 Check **Channels Licensed:** number is correct.

3 Check that there is a **Licensing Record Number:**. This may be needed by Westell support to verify licence validity.

If the number of channels licensed is incorrect, refer to section *4.7.4 Licensing* for details of entering the licence key for the correct number.

4 If everything is correct, select **Submit**; any changes will be confirmed.

5 Select **Close** to return to the main Menu.

3.6.7 Deactivate SCN Ports

1 Select **Configuration**, **SCN** and then **Activate Ports**.

2 Click on the **Out of Service** radio button to deactivate the port or ports.

3 Select **Submit** and the change will be confirmed.

4 Select **Close** to return to the Menu.

3.6.8 Commission Channels

1 Select **Configuration**, **SCN** and then **Commission Channels**.

2 In accordance with the attached PBX or other equipment, check that the correct Channels are ticked for use. Click on the boxes to select or deselect Channels.

3 Select **Submit** and any changes will be confirmed.

4 Select **OK** on the screen warning about losing calls.

5 Select **Close** to return to the Menu.

3.6.9 Set Orientation

The A/B orientation must be set opposite to the orientation of each Port of the PBX or other SCN equipment with which the IiQ Gateway is communicating. Likewise, the X/Y channel priorities must be set opposite to those of the PBX or other SCN equipment with which the IiQ Gateway is communicating.

1 Select **Configuration**, **SCN** and then **Set Orientation**.

2 Set A/B orientation by clicking on the radio button.

3 Set X/Y channel priorities by clicking on the radio buttons.

4 Select **Submit** and any changes will be confirmed.

5 Select **OK** on the screen warning about losing calls.

6 Select **Close** to return to the main Menu.

3.6.10 Configure Level 3

The Port Channel Allocations should be set opposite to that set for the port of the DPNSS PBX with which the IiQ Gateway is communicating.

1 Select **Configuration**, **SCN** and then **Configure Level 3**.

2 For **Channel Allocation**, select **Low to High** or **High to Low** as appropriate for each Port being used.

3 Select **Submit** and the changes will be confirmed.

4 Select **Close** to return to the main Menu.

3.6.11 Reactivate SCN Ports

1 Select **Configuration**, **SCN** and then **Activate Ports**.

2 Click on the radio button to activate the port or ports.

3 Select **Submit** and the change will be confirmed.

4 Select **Close** to return to the main Menu.

3.6.12 Configure Gatekeeper

If the IiQ Gateway is to be used in conjunction with a Gatekeeper, continue as below. If there is no Gatekeeper in the network, and you wish to display a local Route ID on the Diagnostic Overview screen then go to section 3.6.13.

Note: Gatekeeper configuration is not required when using Internal Routing only.

1 Select **Configuration**, **IP** and then **Gatekeeper**.

2 To use automatic Gatekeeper discovery, click on the box alongside **Automatic Discovery (after reset)** or,

To use a specific Gatekeeper, type in the address and Port number in the **Gatekeeper Address (after reset)** field

3 Enter the time in minutes that a registration is allowed to live.

4 Type in a number for the maximum registration attempts.

5 For **Local Route ID:** type in the name or alias by which the IiQ Gateway is to be known to the Gatekeeper. If a **Local Route ID** is configured, it will be displayed on the status bar together with the IP address.

Note: When the **Local Route ID** is changed, screens already opened will continue to display the previous **Local Route ID** or *(Default_local_route_id)* until the page is refreshed.

6 If using a Gatekeeper, enter numbers (E.164 aliases or number prefixes) to register with the Gatekeeper.

7 Select **Submit** and the changes will be confirmed.

8 Select **Close** to return to the main Menu.

3.6.13 Configure Local Route ID

This section is only required if the IiQ Gateway is not connected to a Gatekeeper and you wish a name or alias for the IiQ Gateway to appear on the status bar.

1 Select **Configuration**, **IP** and then **Gatekeeper**.

2 For **Local Route ID:** type in a name or alias.

Note: When the **Local Route ID** is changed, screens already opened will continue to display the previous **Local Route ID** or *(Default_local_route_id)* until the page is refreshed.

3 Select **Submit** and the changes will be confirmed.

4 Select **Close** to return to the main Menu.

3.6.14 Configure Terminal Capabilities

The terminal capabilities are the part of the call signalling procedures that tell the distant endpoint which type of media encoding is supported. **Codec Support** allows the management of bandwidth preferences on a unit-by-unit basis.

Note: The capabilities used on a given call are selected as a result of negotiation between the two endpoints based on the unit's preferences. They cannot be forced simply by setting the capabilities of one end. For example, if the first endpoint codec preference is set to G.711 preferred and G.729a secondary, and the second endpoint is set to G.729a preferred and G.711 secondary, the codec chosen will be G.711 if the first endpoint wins the negotiation. However, if the second endpoint is set to G.729a only, then the codec chosen will be G.729a as this is common for both endpoints. See section 4.3 IP, Terminal Capabilities for further details.

1 Select **Configuration**, **IP**, and then **Terminal Capabilities**.

2 Select and enable the **Codec/s** from the list.

3 To reduce the network bandwidth required by each Codec enabled, select **Silence Suppression**. Samples sent will be reduced when there is no voice activity.

4 Insert the number of **Frames per Packet** to control the number of voice samples collected before forwarding over the network.

Note: A high number increases the delay through the gateway but reduces the IP overhead. A low number will usually give better-perceived voice quality at the expense of slightly greater bandwidth requirements.

5 Set the **Precedence** for each Codec selected.

6 Select **Submit** and the change will be confirmed.

7 Select **Close** to return to the main Menu.

3.6.15 Set Media Control

Media Control is used to configure the various methods and options related to the H.323 signalling aspects of opening a media channel.

1 Select **Configuration**, **IP**, **Media Control**.

2 Enable **Use of Fast Start** will cause the IiQ Gateway to follow the faststart procedures as defined by H.323 and H.225. Assuming the far end unit is also configured to support faststart, this allows the unit to quickly open an audio (media) path at a much earlier stage of the call signalling than normal H.245 procedures allow.

However, additional capabilities, for example DTMF, must be exchanged using normal H.245 procedure.

When **Use of Fast Start:** is **Disabled**, it will cause the IiQ Gateway unit to follow H.245 procedures in order to open a media path.

3 Enable **H.245 Tunnelling:** if you want to cause all H.245 information passed between this unit and the far end unit to be encapsulated in Q.931 signalling messages.

If **H.245 Tunnelling:** is **Disabled**, all H.245 information will be passed as distinct H.245 messages using an independent TCP channel.

4 Enable **Early use of H.245:** if you want this to provide the necessary addressing information required to open a media channel in the SETUP message of the call signalling phase. A separate H.245 TCP channel will be opened by the far end and H.245 negotiation will take place.

If **Early Use of H.245:** is **Disabled**, the H.245 negotiation will not occur until after the H.245 address has been sent in the Connect message.

5 Set the **Master/Slave Determination Timeout:** in seconds. This causes the unit to wait for the specified time before a master/slave determination request has deemed to fail because the request was not acknowledged by the far end unit.

6 Set the **Terminal Capabilities Timeout:** in seconds. This causes the unit to wait for the specified time before a terminal capability set message request has deemed to fail because the message was not acknowledged by the far end unit.

7 Select **Submit** and the changes will be confirmed.

8 Select **Close** to return to the main Menu.

3.6.16 Set Quality of Service

IP networks were primarily developed for data transmission that was not a real-time application. However, as voice is real-time, these settings can help network administrators minimise some of the 'lumpiness' of busy networks that will lead to voice drop-out or delay.

Note: These settings should only be changed from the default values under guidance from your network administrator who can advise on changes and the method to use to suit your particular network.

1 Select **Configuration**, **IP**, **Quality of Service**.

2 Select either **Type of Service** or **Differentiated Services Codepoints**.

3 For **Type of Service**, make relevant changes for your particular network only as instructed by your network administrator or accept the default settings.

For **Differentiated Services Codepoints**, insert the 6 bit string for either or both Media and Call Signalling as instructed by your network administrator.

4 Select **Submit**

5 Select **Close** to return to the main Menu

Some useful information on Quality of Service may be found in *Appendix E2*.

3.6.17 Configure Call Routing

Call routing tables are generated locally on a PC before being uploaded to the IiQ Gateway. This section describes the format for the tables and how to load them. A Route Wizard has been provided to help you create and maintain the Route ID and IP Address tables. See section *4.6 Route Wizard*.

Note: For Internal Routing only, you must set up both Route ID and IP Address tables.

When Internal Routing is used in conjunction with a Gatekeeper, you only need to set up and configure the Route ID table. If both tables are set up and configured, the Gatekeeper will ignore the IP Address table.

Address Range		
Start	**Finish**	**Route Id**
0120	0129	Basingstoke
0130	0199	London
		DefaultRoute
End of Table		

Example Route ID Table

1 Create a Route ID Table in the following text format:

```
version =     1;
//  filename:  rt_conf.txt
//  created:  2002-11-26
//  description:  initial route id table
//  author:  yourname
"0120","0129","Basingstoke";
"0130","0199","London";
"","","DefaultRoute";
//  end of file
```

2 Save the Route ID Table as **rt_conf.txt** in plain ascii text.

Route Id	**IP Transport Addresses**	
	Address	**Port No**
Basingstoke	255.1.254.2	1720
	255.1.254.3	1720
	255.1.254.4	1720
	255.1.254.5	1720
London	253.3.254.4	1720
	253.3.254.19	1720
DefaultRoute	245.6.124.8	1720
End of Table		

Example IP Address Table

3 If not using a Gatekeeper, create an IP Address Table in the text fomat shown on the following page:

```
version =         1;
//  filename:  ip_conf.txt
//  created:  2002-11-26
//  description:  initial ip address table
//  author:  yourname
"Basingstoke",    "255.1.254.2","1720", "255.1.254.3","1720",
                  "255.1.254.4","1720", "255.1.254.5","1720";
"London",         "253.3.254.4","1720","255.3.254.19","1720";
"DefaultRoute",   "245.6.124.8","1720";
//  end of file
```

Note: In the IP Address Table, **IP Route ID** names will be re-ordered into alphabetic order.

4 Save the IP Address Table as **ip_conf.tx**t in plain ascii text.

5 Select **Configuration**, **Call Routing** and then **Upgrade from PC**.

6 For the **Routing Table Configuration File:**, select **Browse** to locate and select the file: **rt_conf.txt**.

7 For the **IP Address Look Up Configuration File:**, select **Browse** to locate and select the file: **ip_conf.txt**.

Note: If there are syntax errors in the file, the upgrade process will be aborted.

8 To confirm the integrity of the file before upgrading, select the **Check** button. If a file is not accepted, check the syntax against the syntax rules specified in sections *4.4.1 Route ID Table* and *4.4.2 IP Address Table.*

Note: When checking the file, the filename field will clear. If necessary go back to Step 7 and reselect the file.

9 If the filename is correct, select **Upgrade**; the data will be loaded in the IiQ Gateway.

10 Select **Close** to return to the main Menu.

3.6.18 Connect E1 Lines

With the Overview Diagnostic screen displayed:

1 Physically connect the E1 telephony lines, ensuring correct Tx and Rx orientation.

2 Refresh the browser screen.

3 Check that the SCN Port(s) field(s) are showing **Port Operational**, as applicable.

3.6.19 Back Up Configuration

The configuration should be backed up to an FTP server for restoring at a later date in the event of a non recoverable system failure.

To back up the configuration:

1 From the main menu, select **Configuration**, **Gateway** and **Back Up Configuration**.

2 Enter the **FTP Server IP Address** onto which the configuration is to be backed up.

3 Enter the **User Name** and **Password** to access the FTP Server.

4 Insert the name of the **Directory** on the FTP Server.

5 Give your back up configuration a file name.

6 Give a brief description of the configuration (this is optional).

7 Select **Back Up** to save the file.

8 When the back up is complete, press **Close** to return to the Main menu.

Note: A configuration can only be restored to an IiQ Gateway running the same software and version as that on the IiQ Gateway from which and when the **Back up Configuration** was made.

3.6.20 Logout

1 Select **Logout** from the main Menu.

2 Confirm that you wish to logout

3 Close the browser window.

The IiQ Gateway is now ready for use.

3.7 Resetting Applications to Defaults

Refer to section *4.1, Reset Application to Defaults* for a list of configuration values that will be reset. SCN values, IP addresses, time and date settings will not be changed:

Should you wish to reset the IiQ Gateway to its default settings:

1 Select **Configuration**, **Gateway** and then **Reset Applications to Default**.

2 Select **Set to Defaults**.

3 Select **Administration** from the top level Menu

4 Select **Reboot the Gateway**.

5 When the unit has rebooted, close the current Browser window and open a new one.

6 Log in again. Refer to section *3.6.3 Login*.

4 Management

This section provides an overview of all configuration and management facilities provided by the Gateway Management Interface.

4.1 Gateway

Set Time & Date

The time and date may be set by typing into the fields provided, accepting the values displayed or by synchronising it with your PC.

Reset Application to Defaults

This allows the user to set the following groups of the IiQ Gateway's configuration parameters back to their default values.

- IP Call Signalling
- IP Gatekeeper
- IP Terminal Capabilities *
- Call Routing Route ID Table *
- Number Translation Table *
- Access Control *
- IP Media Control
- IP Media Gateway *
- IP Quality of Service *
- Call Routing IP Address Table *
- SNMP traps *

No change will be made to the IiQ Gateway's SCN configuration values, date and time settings, software selection, licence key, logs or statistics. The IiQ Gateway must be rebooted for changes to take effect, except those marked with an asterisk which will change dynamically.

Back Up Configuration

When the IiQ Gateway has been satisfactorily configured, this configuration can be backed up to an FTP server for restoring at a later date in the event of a non recoverable system failure. To back up the configuration:

1. From the main menu, select **Configuration**, **Gateway** and **Back Up Configuration**.
2. Enter the **FTP Server IP Address** onto which the configuration is to be backed up.
3. Enter the **User Name** and **Password** to access the FTP Server.
4. Insert the name of the **Directory** on the FTP Server.
5. Give your back up configuration a file name.
6. Give a brief description of the configuration. This is optional.
7. Press Back Up to save the file.
8. When the back up is complete, press **Close** to return to the Main menu.

Restore Configuration

This allows a configuration that has been previously backed up to either be restored to the IiQ Gateway from which it was backed up or be installed on another IiQ Gateway unit.

Note: A configuration can only be restored to an IiQ Gateway running the same software and version as that on the IiQ Gateway from which and when the **Back up Configuration** was made.

To restore a configuration:

1 From the Main Menu, select **Configuration**, **Gateway** and **Restore Configuration**.

2 Enter the **IP Address** of the server containing the back up file.

3 Enter a **User Name** and **Password** for the FTP server.

4 Enter the **Directory** name containing the back up file.

5 Enter the **Name** and extension of the back up file.

6 Click on **Select** and the **Configuration Details** window will appear.

7 Check the **Configuration Details** are correct and compatible with the IiQ gateway that you are restoring to or installing on and select **Install**.

8 When the Restore is confirmed, select **Close**. The IiQ gateway will reboot itself.

Changes will not be made to IP addresses, software selection, licence key, logs or statistics.

Set Addresses

The IiQ Gateway's IP Addresses and Subnet Masks should have been established during the initial setup process. However, it is possible to change these addresses and to insert a **Default Gateway IP Address** for both signalling and media. Leaving the **Default Gateway IP Address** fields blank signifies that no Default Gateway is to be used.

Changes will not be effected until the IiQ Gateway has been reset and it will be necessary to log into the IiQ Gateway with the new address for any further configuration changes.

Configure SNMP Traps

Up to eight **Trap Destination Addresses** may be enabled by inserting the address value. To disable an address, remove the address value.

Traps are grouped as follows:

- Major Alarm
- Reset Traps
- System Events
- Port Errors
- Call Info Traps
- Layer 1 Alarms

To enable a group, check the box as required. To enable all groups select **Enable All**. Select **Submit** to save any changes.

Please refer to *Section 8 SNMP Traps* for the group tables. Links are provided on the Gateway Management Interface page to the MIBs that define the IiQ 2030 Series Gateway traps.

4.2 SCN

Activate Ports

The SCN Ports may be activated or deactivated. Deactivate before changing any SCN settings.

Note: The IiQ Gateway needs to derive its clocks from the PBX. Please refer to section *6 SCN Clock Synchronisation*.

Commission Channels

The Commission Channels configuration determines which of the SCN channels can be used. The licence key determines how many of these channels may be used at any one time. The number of commissioned Channels may be different from the number of licensed Channels.

Refer to section *4.5.4 Licensing* for an explanation of the licence key.

Set Orientation

The A/B orientation must be set opposite to the orientation of each Port of the PBX or other SCN equipment with which the IiQ Gateway is communicating.

Likewise, the X/Y orientation must be set opposite to the orientation of each of the Channels of the PBX or other SCN equipment with which the IiQ Gateway is communicating.

Configure Level 3

The Port Channel Allocations must be set opposite to that set for the port of the PBX with which the IiQ Gateway is communicating.

If Proxy Diversion is enabled and a call from the IP network to the DPNSS network is diverted, the IiQ Gateway will intervene to ensure that the diversion takes place. If Proxy Diversion is not enabled, calls from the IP network encountering diversion at a DPNSS PBX are likely to fail. This setting does not affect calls from DPNSS to either IP or transparently over IP to other DPNSS extensions.

Operator Recall Timeout only applies if **Proxy Diversion Enabled** is selected. If a call from the IP network to an operator in the DPNSS network is diverted, the phone to which it has been diverted will ring for the number of seconds configured and then, if the call has not been answered, the call will revert to the operator. If **Operator Recall Timeout** is set to **0**, the call will remain diverted.

4.3 IP

Gatekeeper

A Gatekeeper is a device that provides a service to look up IP addresses against registered identities (which may be phone numbers). If a remote Gatekeeper or IP Telephony Server is being used, the Route ID Tables need not be configured in the IiQ Gateway.

Gatekeeper Address either displays the gatekeeper address that the IiQ Gateway is configured to use, or indicates that automatic gatekeeper discovery is in use, or indicates that the IiQ Gateway is configured not to use a gatekeeper.

When **Automatic Discovery (after reset)** is selected, after resetting the unit, the IiQ Gateway uses the automatic gatekeeper discovery procedure to register with a gatekeeper . The gatekeeper discovery message (GRQ) will be sent to the RAS multicast address - 224.0.1.41 port 1718

Gatekeeper Address (after reset) is the address including the port number (typically 1719) that the IiQ Gateway will attempt to register with after the IiQ Gateway has been reset. This address is not used if automatic discovery is enabled.

Note: To route calls without using a gatekeeper, **Automatic Discovery (after reset)** must be disabled and the **Gatekeeper Address (after reset)** field must be empty.

Source RAS Port shows the port number that the IiQ Gateway is configured to use for RAS signalling. A 0 indicates that it is not specified.

Source RAS Port (after reset) is the port number that will be used for RAS signalling after resetting the IiQ Gateway. If the precise port number is not important, set this to 0.

Registration Time to Live is the maximum time in minutes that the IiQ Gateway may use the services provided by the Gatekeeper before renewing its registration.

Between 1 and 200 **Maximum Registration Attempts** may be set.

A name for the IiQ Gateway may be set up in **Local Route ID:**. This name is passed to the Gatekeeper at the time of registration and is displayed on the status bar of the management screens together with the IP address.

The IiQ Gateway sends the list of **Registered Numbers** to the gatekeeper when it registers. The gatekeeper uses it to determine which calls to route via the IiQ Gateway to the Switched Circuit Network. Each number is either an E.164 alias or a number prefix.

At least one number must be configured if the IiQ Gateway has been configured to register with a gatekeeper. If the **Registered Numbers** are changed, the IiQ Gateway deregisters from the gatekeeper and registers again, causing a disruption to service. The Diagnostic Overview page will show whether re-registration has succeeded.

Note: Any changes to **Automatic Discovery (after reset)**, **Gatekeeper Address (after reset)** and **Source RAS Port (after reset)** will only be actioned when the IiQ Gateway is reset.

Terminal Capabilities

The terminal capabilities are the part of the call signalling procedures that tell the distant endpoint which type of media encoding is supported. **Codec Support** allows the management of bandwidth preferences on a unit-by-unit basis.

The capabilities used on a given call are selected as a result of negotiation between the two end-points based on the unit's preferences. They cannot be forced simply by setting the capabilities of one end.

Codec type determines the compression algorithm employed. If the codec is **Enabled** it is included in the terminal capability set sent to the distant endpoint. If it is disabled it is removed from the list.

Enabling **Silence Suppression** will reduce the network bandwidth required by the codec by reducing the samples sent when there is no voice activity.

The **Frames per Packet** parameter controls how many voice samples are collected before being forwarded over the network. A high number increases the delay through the gateway but reduces the IP overhead. A low number will usually give better-perceived voice quality at the expense of slightly greater bandwidth requirements.

The number of frames per packet is a trade-off between network bandwidth utilisation and packetisation delay (which is highly dependent on the codec selected for the call) voice and is a network design decision. In a typical VoIP network each RTP packet might be expected to carry 20 or 30 ms of voice.

With the G.729 codec each frame carries 10ms of encoded voice; with the G.711 codec each frame carries 1 ms of voice. So to achieve 20 or 30 ms of signal per packet for G.711 codecs one would set the Frames per Packet parameter to 20 or 30 while for G.729 the value would be set to 2 or 3.

The IiQ Gateway will use a codec in order of **Precedence,** where 1 is first.

The IiQ Gateway supports T.38 fax services. Tick the **T.38 Enabled** box and when the IiQ Gateway unit recognises a fax call it switches to T.38 mode, provided the other node in the system has T.38 capability. If **T.38 Enabled** is not set or the other node does not have T.38 compatibility, the IiQ Gateway will switch to G.711 codec pass-through mode, provided the G.711 Codec is supported by both itself and the other node.

DTMF Support: If **RFC2833 is Enabled** and the remote endpoint is also RFC2833 capable, DTMF tones are transmitted in the media streams RTP headers. This is the most reliable method and should be used by default. Some endpoints however (notably Microsoft Netmeeting©) will fail calls if this feature is enabled and so it must be disabled in the menu.

Media Control

Use of **Fast Start**, **H.245 Tunnelling** and **Early Use of H.245** may each be enabled or disabled.

If **T.38 Fax** is enabled (see *Terminal Capabilities*) together with the use of **Fast Start**, **H.245 Tunneling** should also be enabled to ensure strict conformance to the H.323 specification. However the IiQ Gateway will function without **H.245 Tunnelling** enabled.

Timeout for **Master/Slave Determination Timeout** and **Terminal Capabilities Timeout** may be set in Seconds.

Quality of Service

Choose between **Type of Service** and **Differentiated Services Codepoints**.

Type of Service configuration options are:

Precedence (category from highest to lowest):

7 - Network Control

6 - Internetwork Control

5 - CRITIC/ECP

4 - Flash Override

3 - Flash

2 - Immediate

1 - Priority

0 - Routine

Delay - Normal or Low

Throughput - Normal or High

Reliability - Normal or High

Differentiated Services Codepoints requires the insertion of a 6 bit string. This should only be changed under the guidance of the Network Administrator.

For more information please refer to *Appendix E2 Quality of Service.*

Call Signalling

H.323 messaging associated with setting up and tearing down a telephone connection is configurable.

When **Suppress Connected Party Number** is ticked, the connected party number information element is omitted from Q.931 connect messages sent to the IP network. Connected Party Number should not normally be suppressed, but calls to some IP servers (e.g. some versions of Cisco Call Manager) will fail if **Suppress Connected Party Number** is not ticked.

Overlap Signalling may be enabled or disabled. The inter-digit timeout may be set in seconds from 0-30. It ensures overlap calls from the SCN can be forwarded en-bloc to the IP.

Overlap Signalling should normally be enabled. However, certain IP gatekeepers and servers (e.g. some versions of Cisco Call Manager) are not able to receive overlap calls; any such equipment on the network should have **Overlap Signalling** disabled and an inter-digit timeout of 3 seconds is recommended.

Inter-Digit Timeout may be set in seconds from 0-30.

Port Range shows the range of ports the IiQ Gateway is configured to use for initiating outgoing call signalling.

Port Range (after reset) is the port range which will be used after the IiQ has been reset. The range should include at least twice as many ports as the number of licensed channels.

Media Gateway

Media Gateway provides a conversion between switched circuit voice channels and IP. Configuration options are:

Enable/Disable Echo Cancellation to each SCN Port.

Echo Cancellation Span in Milliseconds for each SCN Port.

RTCP Sender Report Interval in seconds.

These settings should only be changed from the default values under guidance from Technical Support who can advise on changes to these settings to suit your particular network.

Media Gateway Tuning

IP networks were primarily developed for data transmission that was not a real-time application. However, as voice is real-time, these settings can help network administrators minimise some of the 'lumpiness' of busy networks that will lead to voice drop-out or delay.

These settings should only be changed from the default values under guidance from Technical Support who can advise on changes to these settings to suit your particular network.

4.4 Call Routing

In order to carry calls over the IP Network, the number needs to be routed to an IP Address and Port ID. To enable routing without an external Gatekeeper, the SCN side of the IiQ Gateway manages this in two stages. The number is first routed to an IP Route ID and then to an IP Address and Port ID.

A Route Wizard has been supplied to aid in setting up the Route ID and IP Address Tables. Please refer to section *4.6 Using Route Wizard*.

Two tables must be set up so that the IiQ Gateway can make these translations:

- Route ID Table
- IP Address Table

The destination IP Address to which a call is routed may be selected by:

- using the internal routing tables if a matching entry is configured for the called number and there is a corresponding entry in the IP Address Table, or by
- making a RAS request to the Gatekeeper if one is configured, or by
- a combination of the above where the destination Route ID alias is selected from the internal tables but the IP Address is resolved using the configured Gatekeeper.

If a Gatekeeper address is configured, all calls are subject to admission control via that Gatekeeper. Therefore, any entries in the IP Address Table would be ignored and the Gatekeeper would be expected to resolve the IP Address.

The table on the facing page shows the criteria used for selecting the routing method for each call:

Gatekeeper Address Configured	Route ID Table	IP Address Table	Call Routing Behaviour
No	Matching Entry	Matching Entry	Route call to IP Address from table.
No	Matching Entry	No Match	Call cannot proceed.
No	No Match	Don't Care	Call cannot proceed.
Yes	Matching Entry	Don't Care	Forward called number and Route ID alias from table to the Gatekeeper via RAS for IP Address resolution.
Yes	No match	Don't Care	Forward called number to the Gatekeeper via RAS for IP Address resolution.

Selecting the Call Routing Method

Alternative Routing

Up to four IP Addresses may be configured for each Route ID. If more than one IP Address is configured and the call setup request to the initially selected destination IP Address fails, a call setup request will be sent to one of the other addresses. The order in which the IP Addresses are selected is determined by the configuration; see section *4.4.2 IP Address Table*.

4.4.1 Route ID Table

A Route Wizard has been supplied on the CD ROM to aid in setting up the Route ID and IP Address Tables. Please refer to section *4.6 Using Route Wizard*.

Address Range		
Start	**Finish**	**Route Id**
0120	0129	Basingstoke
0130	0199	London
		DefaultRoute
End of Table		

Example Route ID Table

The **Address Start** and **Finish** columns specify a wildcard terminated range; for example, the entries 0120 and 0129 implies all addresses starting with 0120, 0121, 0122 and so on up to 0129.

A blank entry in the **Address Start** and **Finish** columns is a 'catch all' wildcard; an address which does not match any other entry in the table will be routed as specified in that wildcard entry.

The Route ID Table above would need to be expressed in the following ascii text format:

```
version = 1;
   //  filename:  rt_conf.txt
   //  created:  27-06-02
   //  description:  initial route id table
   //  author:  yourname
   "0120","0129","Basingstoke";
   "0130","0199","London";
   "","","DefaultRoute";
   //  end of file
```

The table is then saved for loading into the Gateway using the Call Routing **Upgrade from PC** or **Upgrade from FTP Server** management pages.

Syntax Rules for the Route ID Table file

The text file shall consist of a Version ID and Route ID entries.

Comments shall follow // characters to the end of the line.

Space characters shall be insignificant.

Version shall be a numeric value between 0 and 4096.

Each Route ID entry shall have the following fields: Address Start, Address Finish, and IP Route ID.

Address Start shall be a numeric digit string of size range 0 - 16 digits.

Address Finish shall be a numeric digit string of size range 0 - 16 digits.

IP Route ID shall be a string of size range 0 - 25 alphanumeric characters.

Fields shall be enclosed between double quotes.

Fields shall be separated by a comma.

The maximum number of Route ID entries is 1000.

Version ID and each Route ID entry shall be terminated with a semicolon.

4.4.2 IP Address Table

A Route Wizard has been supplied on the CD ROM to aid in setting up the Route ID and IP Address Tables. Please refer to section *4.6 Using Route Wizard*.

Route Id	IP Transport Addresses	
	Address	Port No
Basingstoke	255.1.254.2	1720
	255.1.254.3	1720
	255.1.254.4	1720
	255.1.254.5	1720
London	253.3.254.4	1720
	253.3.254.19	1720
DefaultRoute	245.6.124.8	1720
End of Table		

Example IP Address Table

The IP Address Table illustrated above would need to be expressed in the following ascii text format:

```
version =        1;
//  filename:  ip_conf.txt
//  created:  2002-11-26
//  description:  initial ip address table
//  author:  yourname
"Basingstoke",   "255.1.254.2","1720", "255.1.254.3","1720",
                 "255.1.254.4","1720", "255.1.254.5","1720";
"London",        "253.3.254.4","1720","255.3.254.19","1720";
"DefaultRoute",  "245.6.124.8","1720";
//  end of file
```

The table is then saved for loading into the Gateway using the Call Routing **Upgrade from PC** or **Upgrade from FTP Server** management pages.

Syntax Rules for the IP Address Table file

The text file shall consist of a Version ID and IP Address entries.

Comments shall follow // characters to the end of the line.

Space characters shall be insignificant.

Version shall be a numeric value between 0 and 4096.

Each IP Address entry shall have the following fields: IP Route ID, IP Addresses, and Port IDs. Each entry shall have at least one IP Address and Route ID and may have up to a maximum of four

IP Route ID shall be a string of size range 0 - 25 alphanumeric characters.

IP Address shall be a numeric digit string of the form:
<1 to 3 digits>.<1 to 3 digits>.<1 to 3 digits>.<1 to 3 digits>. Each section of the number can have a value in the range 0 - 255.

Port ID shall be a numeric digit string of value in the range 0 - 65535.

Fields shall be enclosed between double quotes.

Fields shall be separated by a comma.

The maximum number of IP Addresses shall be 1000

The Version ID and each IP Address entry shall be terminated with a semicolon.

Configure

IP Load Sharing is part of the Alternative Routing feature of the IiQ Gateway. If the initial call attempt fails, the IiQ Gateway will select the next IP address in the table and attempt the call again. This continues until either the call succeeds or all entries in the IP Address Table have been exhausted.

When **IP Load Sharing** is enabled, the IiQ Gateway will pick a destination IP Address at random from the entries in the IP Address Table associated with the chosen route. The result is that where a destination is served by two or more gateways, incoming calls will be evenly distributed between them.

When **IP Load Sharing** is disabled, the IiQ Gateway will try each IP Address in the order which they appear in the IP Address Table. This facility can be employed to test network routing during configuration as the destination IP Address can always be determined.

Upgrade from PC

Enables you to search for and import the Route ID Table and IP Address Table files created.

Note: The upgrade process will be aborted if there are syntax errors in the file. However, the integrity of the file may be confirmed before upgrading by selecting the **Check** button. If a file is not accepted, the syntax should be checked against the rules specified above.

Upgrade from FTP Server

Enables you to import the Route ID Table file and IP Address Table file via an FTP server.

The IP address of the FTP server, a User Name and a Password are all required to access the FTP server. The directory and filenames of the configuration files on the FTP server are also required.

The files specified for the FTP transfer must be a filenames of no more than 8 characters with a filetype of no more than 3 characters (DOS 8.3 format).

Care should be taken when specifying path names. DOS path names require a back slash (\), UNIX path names require a forward slash (/).

Note: The upgrade process will be aborted if there are syntax errors in the file. However, the integrity of the file may be confirmed before upgrading by selecting the **Check** button. If a file is not accepted, the syntax should be checked against the rules specified above.

Display Route ID Table

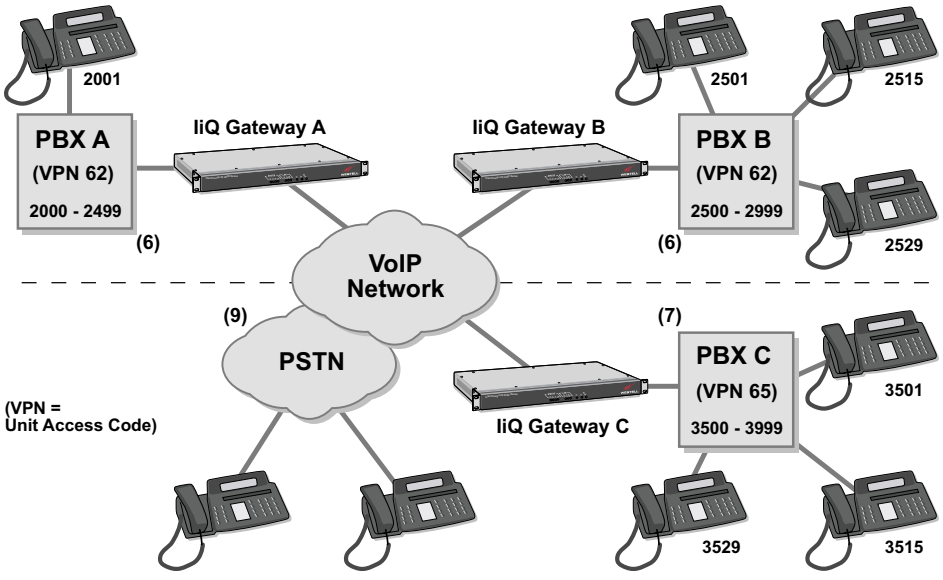
Details of the Route ID Configuration are displayed.

Display IP Address Table

Details of the IP Address Configuration are displayed.

4.5 Number Translation

Number Translation may be required when the sender or receiver of protocol is in a different addressing domain than the IiQ Gateway. It allows addressing information entering or leaving the IiQ Gateway to be normalised to a numbering scheme appropriate to the recipient.



Communicating Between VPNs Across an IP Network.

The example illustration shows a typical layout for an organisation that may have two PBXs sharing the same VPN (62) and another with its own VPN (65).

With Number Translation, when a caller connected to PBX-A places a call to a recipient connected to either PBX-B or PBX-C, the address will be translated by IiQ Gateway A to enable the number to be recognised by the correct IiQ Gateway (B or C).

This receiving IiQ Gateway will then translate the number to an address recogniseable to the PBX it serves, enabling it to direct the call to the recipient.

In this example, if the recipient is connected to a PBX on the same VPN, only the recipient's number is required but if the recipient is connected to a PBX on a different VPN, a digit can be added before the recipent's number to route the call to the correct PBX. This is the basis of and purpose for setting up Number Translation.

Number Translation Tables must be created in order that the Caller IiQ Gateway can recognise specified digits in the address to remove and or add digits accordingly.

When a caller at number 2001 wishes to connect with number 2529, the call needs to be routed through IiQ Gateway A, across the IP Network and through IiQ Gateway B. As this is on the same VPN (62), IiQ Gateway A will interrogate the table, remove 0 digits from the start of the number and then add 62 to the start of the number, thus routing the call through IiQ Gateway B.

When a caller at number 2001 wishes to connect with number 3515, the call needs to be routed through IiQ Gateway A, across the IP Network and through IiQ Gateway C. As this is on a different VPN (65), IiQ Gateway A will require an additional number to be able to transparently route the call through IiQ Gateway C. By allocating an extra digit (e.g.7) to the start of the number, when the IiQ Gateway interrogates the table and finds 7 at the start of the address, it will remove the first digit and add 65, thus routing the call through IiQ Gateway C.

When a caller at number 2001 wishes to place an external call over the PSTN, by allocating an extra digit (e.g. 9) to the start of the number, IiQ Gateway A will remove the first digit and add nothing, thus routing the call through the IP Network's gateway to the PSTN system.

In the event that a recipient has diverted calls to another number, this information needs to be relayed back to the caller and the table should therefore include number translations for both outgoing and incoming connections.

Note: Number Translation is applied to called party numbers, calling party numbers and connected party numbers.

The Number Translation Table contains ingress entries relating to incoming calls and egress entries relating to outgoing calls passing through the SCN port of the IiQ Gateway. The ingress number translation occurs before call routing and the egress number translation occurs after call routing.

Each IiQ Gateway must be configured similarly, but the same table would not be appropriate.

Direction	Address	Translation	
	Match Digits	Remone 'n' Digits	Prepend Digits
Ingress	7	1	65
Ingress	9	1	
Ingress	0	0	62
Egress	65	2	7
Egress	62	2	
Egress		1	9

Example Number Translation Table.

The Number Translation Table illustrated on the previous page would need to be expressed in the following ascii text format:

```
version =     1;
//  filename:  ad_conf.txt
//  created 27-06-02
//  description:  initial Number Translation table
//  author:  yourname
ingress,"7",1,"65";
ingress,"9",1,"";
ingress,"0",0,"62";
egress,"65",2,"7";
egress,"62",2,"";
egress,"",1,"9";
//  end of file
```

and then saved for importing using **Upgrade from PC**.

Entries in the Address column are wildcard terminated; for example, 65 implies all addresses starting with the digits 65. A null entry in the Address column is a catch all wildcard; an address which does not match any other entry in the table will be subject to the translation specified in the null address entry.

Note: If Number Translation is enabled, a call will fail if the number does not match an entry (ingress or egress) in the relevant table. To specify that non matching numbers should not be translated, include a null entry in each section (ingress and egress)to remove 0 digits and prepend 0 digits.

Syntax Rules for the Number Translation Configuration file

The text file shall consist of a version id and Number Translation entries.

Comments shall follow // characters to the end of the line.

Space characters shall be insignificant.

Version id shall be a numeric value between 0 and 4096.

Each Number Translation entry shall have the following fields: Direction, Match Digits, Remove 'n' Digits, Prepend Digits .

Direction may be ingress or egress.

Match Digits shall be a numeric digit string of size range 0 - 16 digits.

Remove 'n' Digits shall be a numeric value in the range 0 - 31 and 255. 255 is to remove all existing digits.

Prepend Digits is a numeric string of size range 0 - 31.

The maximum number of Number Translation entries allowed shall be 40 of which up to 20 may be ingress and up to 20 may be egress.

The **Match Digits** and **Prepend Digits** fields shall be enclosed between double quotes.

Fields shall be separated by a comma.

Each Number Translation entry shall be terminated with a semicolon.

Configure

Allows Number Translation to be enabled or disabled.

Upgrade from PC

Allows the Number Translation table to be changed by loading a text file to the IiQ Gateway. The file must be created in ASCII text outside the Web browser and must be in the exact format specified in the User Guide. The file can then be located and loaded using the Gateway Management Interface.

If the format of the file is incorrect, the file cannot be loaded. The file can be verified using the **Check** button before selecting **Upgrade**. An attempt to load an incorrect file will be rejected and the previous configuration will remain unchanged.

Upgrade from FTP Server

Allows the Number Translation Table to be changed by loading a text file from an FTP server to the IiQ Gateway. The file must be created in ASCII text outside the Web browser and must be in the exact format specified in this User Guide.

The IP address of the FTP server, a User Name and Password (to access the FTP server) and the directory and file name of the new configuration file on the FTP server must be typed in, then select **Upgrade**.

If the format of the file is incorrect, the file cannot be loaded. The syntax of the file can be verified using the **Check** button before selecting **Upgrade**. An attempt to load an incorrect file will be rejected and the previous configuration will remain unchanged.

Display

Details of the Number Translation Configuration are displayed.

4.6 Using Route Wizard

Route Wizard Professional Edition is a standalone application intended primarily for use under Microsoft Windows®. It requires Java Run Time Environment v1.4.1_02 or later which may be downloaded from the Sun Web site. For more information, please refer to the Route Wizard Help file (*rwhelp.htm*) included on the CD ROM with this manual.

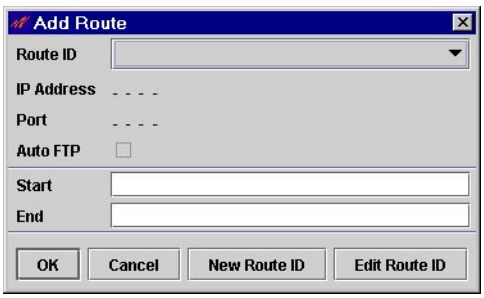
Call Routing

To use the Route Wizard to create Route ID and IP Address tables:

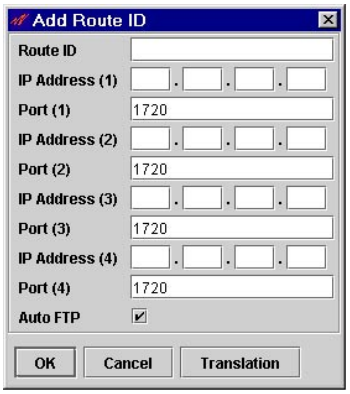
1 Double click on **RouteWizard.jar**

2 Go to **File**, **New routing table**.

3 Go to **Edit**, **New entry**. A window similar to the following will appear:



4 Select **New route ID**. A window similar to the following will appear:



5 Enter a name for the **Route ID**.

6 Enter one or more addresses in the **IP Address** fields.

7 Make sure that the ports are set to 1720 and that **Auto FTP** is checked. Select **OK**

8 Check that the name inserted appears alongside Route ID and insert the **Start number**.

9 Insert the **End** number and select **OK**.

10 Repeat steps 3 to 9 until you have included the information for all Route IDs.
Note: A Route ID may be used in more than one table entry.

11 The **RouteWizard** window will show the complete list of entries.

12 Go to **File**, **Save Routing Tables**.

13 Browse to a suitable location, enter a file name and select **Save**.

The following files will be saved:

- Route ID table with extension .RID
- IP Address table with the extension .IPA
- An executable batch file with the extension .BAT

14 Execute the .BAT file and the routing tables will be installed on all IiQ Gateway units of IP Addresses listed.

For a more detailed explanation on using the Route Wizard, see the Wizard tutorial file (*rwtutor.htm*) included on the CD ROM with this manual.

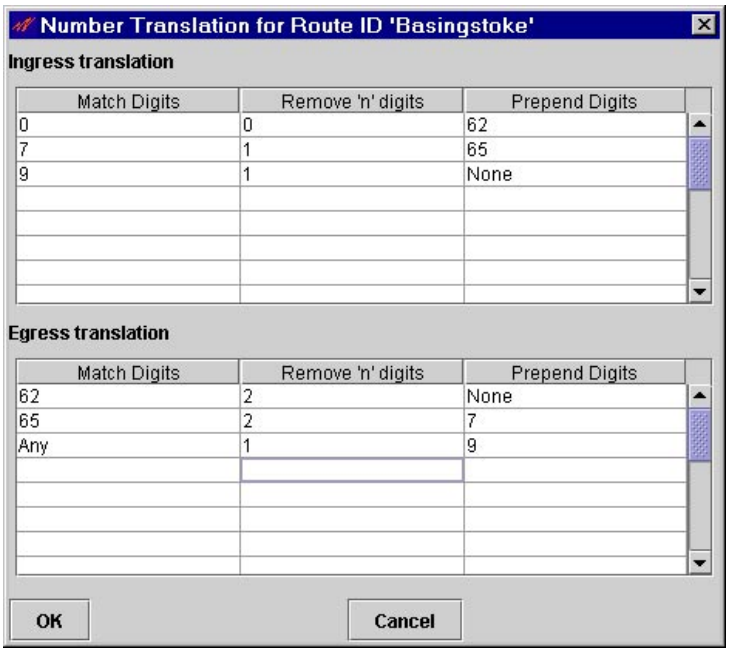
Call Routing and Number Translation

Not many applications will require Number Translation tables. However, should an application require them, it is recommended that the Route Wizard is used to create them.

To use Route Wizard to create Route ID, IP Address and Number Translation Table:

1 Follow the procedure from 1 to 6 as shown in **Call Routing** above.

7 Make sure that the ports are set to 1720 and that **Auto FTP** is checked. Select **Translation**. The Number Translation window will appear:



8 For **Ingress translation**, insert numeric values for **Match Digits**, **Remove 'n' Digits** and **Prepend Digits** (refer to section 4.5 for syntax rules).

9 For **Egress translation**, insert numeric values for **Match Digits**, **Remove 'n' Digits** and **Prepend Digits**. Select **OK**.

10 At the **Add Route ID** window, select **OK** again and check that the name inserted appears alongside **Route ID** in the **Add Route** window.

11 Insert the **Start** and **End** numbers and select **OK**.

12 Repeat steps 3 to 11 until you have included the information for all Route IDs.
Note: A call will fail if the called party number or calling party number does not match an entry in the relevant ingress and egress table. If necessary, add an 'Any' entry as shown above.

13 The **RouteWizard** window will show the complete list of entries.

14 Go to **File**, **Save Routing Tables**.

15 Browse to a suitable location, enter a file name and select **Save**.

The following files will be saved:

- Route ID table with extension .RID
- IP Address table with the extension .IPA
- An executable batch file with the extension .BAT
- A Number Translation table named xlat.ATR for each Route ID.

16 Execute the .BAT file and the routing tables will be installed on all IiQ Gateway units of IP Addresses listed.

The Number Translation table for each IiQ Gateway unit can be checked using the Gateway Management Interface by going to **Configuration**, **Number Translation**, and then **Display**.

For a more detailed explanation on using the Route Wizard, see the Wizard tutorial file (*rwtutor.htm*) included on the CD ROM with this manual.

4.7 Administration

To access Administration functions, Advanced Access is required.

4.7.1 Access Control

Access Control settings allow the user passwords and **Non-Use Timeout Period** to be set. Alpha-numeric characters with the exception of space are legal for passwords. The **Non-Use Timeout Period** is the time allowed for a user to be logged into the Gateway Management Interface without actively using it before being automatically logged out when another user attempts to Login.

4.7.2 Software Upgrade

The IiQ Gateway is supplied with an embedded default operational software. It can only be upgraded with software that is of the same type as the embedded software.

Software Upgrade allows a new version of the software application to be downloaded to the IiQ Gateway using an FTP server.

The IP address of the FTP server, a User Name and a Password are all required to access the FTP server. The directory and filename of the new application on the FTP server is also required. Selecting **Upgrade** will download the new application to the IiQ Gateway.

This new application will overwrite an existing previously downloaded application but not the default application. The new application will run next time the IiQ Gateway is reset, but only if the new software has been selected using the **Software Selection** facility. Instructions on installing the software version will be provided with the new software.

Configuration Back-Ups

Configuration back-ups are release specific. Once the software upgrade has completed successfully and is operational on the unit, a new configuration back-up should be saved.

The procedure is as follows:

1. Upgrade to the new version of the software.
2. Select the version of the software to run next time the unit is restarted.
3. Restart the IiQ Gateway unit. The configuration stored on the unit is automatically loaded into the new version of software.
4. Perform a Back-Up Configuration as described in section *3.6.19 Back Up Configuration*. A configuration back-up file compatible with the newly activated software is produced.

Note: It is not possible to restore a backed up configuration file to a system running a different version of software to that under which the back up file was saved.

Note: It is recommended that each back up configuration file is given a unique name which includes the software release number. This will ensure that if the configuration back up files are stored in a central location, then a new back up file does not overwrite an existing file which may be required for a different location.

4.7.3 Software Selection

The IiQ Gateway is supplied with an embedded default operational software.

Software Selection provides a choice between using the new software downloaded or the embedded default software supplied with the IiQ Gateway.

4.7.4 Licensing

The Licensing screen displays **the Product Variant**, the **Maximum Channels** available in that variant, the current number of **Channels Licensed** and the **Licensing Record Number**.

Only product variants that support Licensing (IiQ 2031EL and IiQ 2032) will display the current **Licence Key** and will permit a new Licence Key to be entered.

To enable more Channel Licences for your IiQ Gateway, you will need to contact your supplier. The following information will be required:

- The IiQ Gateway's serial number
- Your authority to purchase
- A contact fax number or e-mail address

On receipt of your Licence Key:

1. From the Main menu, select **Administration** and then **Licensing**.
2. Overwrite the existing **Licence Key** entry with the key supplied.

   Note: If an incorrect key is entered, an error warning will be displayed. Re-enter the key and resubmit. If the problem persists, contact your supplier.
3. Select **Submit** and the change will be confirmed.
4. Select **Close** to return to the Main menu.
5. Refresh the screen using the browser menu and the new information will be displayed.

When a new Licence key has been entered the number of SCN channels that can be used at any one time changes. The SCN Commission Channels configuration may also need to be changed, to make all the required channels available, refer to sections *4.2* and then *3.6.8*.

Note: If an incorrect Licence Key is entered the previous licence remains effective. If an incorrect Licence Key is entered 5 times, no further Licence Key entry is accepted until the IiQ Gateway has been rebooted.

The **Hardware Serial Number** is also displayed, which must be quoted when buying a new licence from the supplier.

4.7.5 Reboot the Gateway

Selecting **Reboot the Gateway** will immediately halt and restart the the IiQ Gateway.

Note: This action is service affecting. Calls in progress will be lost and service will be interrupted until the IiQ Gateway is fully operational again.

5 Diagnostics

The Gateway Management Interface produces logs for System, SCN Port and SCN Major Alarm.

Information in management diagnostics screens may be printed or by using the **Select All**, **Copy** and **Paste** facilities in the Web browser, may be exported in ascii text to other applications.

Note: If the Flash memory is formatted or the system is set to Factory Defaults, all of the logs will be cleared and the information will be lost. Other than the System Log, when the system is rebooted, all other logs will be cleared.

5.1 General

5.1.1 System Log

The system log is created and updated dynamically and records the date and time of certain system events, including system crashes, automatic reboots and manual restarts. Successful and attempted logins are recorded.

The table on the following pages defines the various events that may be generated by the IiQ Gateway and written to the System Log during operation. Events are classified to indicate their seriousness which consist of four levels:

- Critical
- Major
- Minor
- Informational.

Critical indicates an event that has caused the IiQ Gateway to restart. These events should always be reported to your supplier. Error codes for critical events are 1, 2, 303 and 601.

Major indicates an event that will cause calls to fail. In some cases, remedial action is possible and should be attempted before contacting your supplier.

Minor indicates an event that may have caused a single call or few calls to fail.

Informational indicates an event that contains information that may be useful but does not require any action.

The table is presented in order of error code number.

Error Code	Log Description	Seriousness	Meaning	Automatic Action	User Action
1	Internal error, Gateway will reboot	Critical	A software error has occurred from which the Gateway could not recover.	The Gateway restarts and an entry is writen to the log.	Report problem to your supplier.
2	Watchdog timeout	Critical	A software error has occurred from which the Gateway could not recover.	The Gateway restarts and an entry is writen in the log.	Report problem to your supplier.
202	H.323 Call Control. Non-symmetric CODEC for call	Minor	The Gateway has received a request to use different codecs in the forwards and backwards direction of the call. This functionality is not supported.	An entry is written to the log.	Check configuration of codecs in the network. If this does not solve the problem, contact your supplier.
202	H.323 Call Control. No matching CODEC for call	Minor	The Gateway and other H.323 endpoint do not have compatible codecs.	Silence is heard in the ear-piece, the call is not cleared. An entry is written to the log.	Check configuration of codecs in the network. If this does not solve the problem, contact your supplier.
202	H.323 Media Control. Cannot switch to G.711 for fax, no matching CODECS	Minor	The other H.323 endpoint does not support fax-capable codecs.	An entry is written to the log.	Check configuration of codecs in the network. If this does not solve the problem, contact your supplier.
291	Received gatekeeper reject message (GRJ)	Major	The Gateway failed to discover a gatekeeper. The reason for the reject is indicated in the log.	An entry is written to the log.	Check the Gateway's configuration relating to gatekeepers. Check that the gatekeeper is set up correctly.
291	Gatekeeper registration request failed	Major	The Gateway failed to register with a gatekeeper. The reason is indicated in the log.	An entry is written to the log.	Check the Gateway's configuration relating to gatekeepers. Check that the gatekeeper is set up correctly.
291	Registered with gatekeeper	Informational	The Gateway has successfully registered with a gatekeeper.	An entry is written to the log indicating the IP address of the gatekeeper.	None
291	Gatekeeper registration request rejected	Major	The Gateway failed to register with the gatekeeper. The reason is indicated in the log.	An entry is written to the log.	Check the Gateway's configuration relating to gatekeepers. Check that the gatekeeper is set up correctly.
302	MG system error: *any other text*	Major	Fault with media (DSP farm).	An entry is written in the log.	Report problem to your supplier.
303	MG system error: *any other text*	Critical	Fault with media (DSP farm).	The Gateway restarts and an entry is written to the log.	Report problem to your supplier.
400	System is starting	Informational	The Gateway has restarted due to power on, or software error or reboot requested by user.	An entry is written to the log and an SNMP trap is generated.	None
600	Reboot requested by user	Informational	The user has requested that the Gateway is restarted.	The Gateway restarts, an entry is written to the log and an SNMP trap is generated.	None
601	Recovered from SCN fatal error	Critical	A software error has occurred that the Gateway could not recover from.	The Gateway restarts and an entry is written to the log.	Report problem to your supplier.
602	The application configuration has been reset to default values	Informational	The user has requested that the Gateway's configuration is reset to factory default.	The configuration is reset to factory default, an entry is written to the log and an SNMP trap is generated.	None

Error Code	Log Description	Seriousness	Meaning	Automatic Action	User Action
603	A user has logged into Web management	Informational	The IP address of everyone who has logged into the Gateway's management system is recorded.	An entry is writen to the log and an SNMP trap is generated.	None.
604	A user has logged out of Web management	Informational	Everyone who has logged out of the Gateway's management system is recorded.	An entry is writen to the log and an SNMP trap is generated.	None.
605	A user has failed to log into Web management	Informational	A log in attempt to the Gateway has failed.	An entry is writen to the log and an SNMP trap is generated.	None.
608	Automatic reboot after restoring configuration from back up file	Informational	Configuaration has been successfully restored from a back up file.	The Gateway's configuration is changed, an entry is written to the log, an SNMP trap is generated and the Gateway restarts.	None.
609	failed to restore configuration from back up file	Minor	Corruption in configuration file or attempting to restore to a different software revision.	An entry is writen to the log and an SNMP trap is generated.	Check that the software revision of the Gateway and configuration file match. If this does not solve your problem, contact your supplier.
610	System date/time set	Informational	The Gateway's date and time has been changed using the Web management.	An entry is written to the log.	None.
816	System date/time set from craft menu	Informational	The Gateway's date and time has been changed using the Craft menu.	An entry is written to the log.	None.

5.1.2 System Details

System Details provide hardware and software information for Gateway and Media Sections of the IiQ Gateway unit.

This information will be required when communicating with the Helpdesk for support .

5.2 SCN

5.2.1 Port Error Logs

Logs are created dynamically for each SCN Port. For each error, the log records the **Date**, **Time** and a brief **Description**.

The log for any port may be cleared using the button provided. Data cleared cannot be recovered and you may wish to print or export this information as ascii text as described at the start of this section.

5.2.2 Major Alarm Log

The SCN **Major Alarm Log** records the **Date**, **Time** and a **Description** of hardware errors.

The log may be cleared using the **Clear** button provided. Data cleared cannot be recovered and you may wish to print or export this information as ascii text as described at the start of this section.

5.2.3 Port Error Statistics

For each Port, SCN **Port Error Statistics** records the number of each of the following error types:

- Framing
- Loss of Synchronisation
- Loss of Signal
- Receiving RAI
- Receiving and Transmitting AIS
- Positive and Negative Frame Slips
- Degraded and Errored Seconds.

The statistics for any port may be cleared using the button provided. Data cleared cannot be recovered and you may wish to print or export this information as ascii text as described at the start of this section.

5.2.4 Call Statistics

For each Port, SCN **Call Statistics** records the number of each of the following call types:

- Current and Peak Active Calls
- Incoming and Outgoing Voice Calls
- Total Incoming and Outgoing Calls
- Incoming and Outgoing Collisions

Statistics may be cleared using the button provided. Data cleared cannot be recovered and you may wish to print or export this information as ascii text as described at the start of this section.

5.3 IP

5.3.1 Codec Usage Interval Statistics

The gateway maintains a log of historical CODEC use for up to 24 hours. CODEC use is shown for each 15 minute time interval for a maximum of 96 of the most recent intervals. The time shown is the start of the 15-minute time interval. The counts show the average and maximum number of CODECs concurrently in use during the interval. The following codec usage statistics are recorded:

- G711 Maximum
- G711 Average

- G729 Maximum
- G729 Average
- T38 Maximum
- T38 Average

The reset button will clear all entries from the log and re-start logging. Data cleared cannot be recovered and you may wish to print or export this information as ASCII text as described at the start of this section. Note that no information will be available until 15 minutes (one complete interval) has elapsed since reset.

5.3.2 Codec Usage Maximum Statistics

These show the maximum (peak) number of CODECs that have been used concurrently since the mechanism was last reset. The following peak codec usage statistics are recorded:

- Peak G711
- Peak G729
- Peak T38

The reset button zeros the values and resets the time and date to the current time and data. Data cleared cannot be recovered and you may wish to print or export this information as ASCII text as described at the start of this section.

5.4 Ping

You can check if any particular IP addresses are accessible from the IiQ Gateway by entering an **IP address to Ping from the IiQ Main Gateway** and/or an **IP address to Ping from the Media Gateway** and then selecting **Submit.** The results will display on screen.

To successfully Ping an IP address on a different LAN segment, the correct Default Gateway Address must be configured both in the IiQ Gateway and in the target equipment.

Note: The Default Gateway Addresses of the IiQ Main Gateway and of the Media Gateway are configured separately.

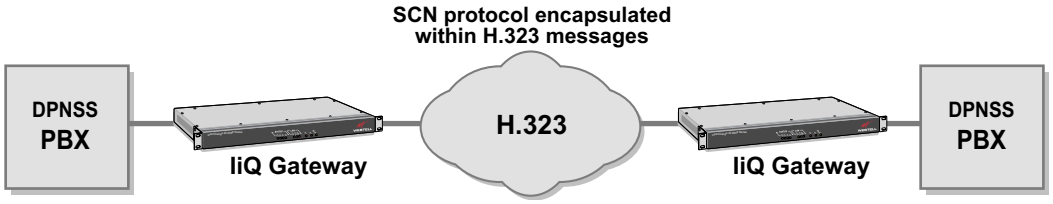
6 Transparent Signalling

6.1 Overview

The IiQ Gateway supports end to end transparent signalling between PBXs via an intervening H.323 Network

Transparency over H.323 allows call control and supplementary service signalling to be carried from an SCN via an intervening IP network to another SCN. The intervening network and IiQ Gateway units simulate a single transit mode in the network.

For transparency over H.323, the IiQ Gateways use H.450.1 generic functional transport signalling. This provides a framework within which communicating IiQ Gateways are able to exchange manufacturer specific information without causing problems in the intervening equipment.



DPNSS or Q.931 over H.323 Transparency.

The figure above shows how, once the call leaves the IiQ Gateway, the transit across the intervening network is handled entirely by that network. It is not necessary for the PBX to provide information about the call further than the IiQ Gateway. The routing functions of the central network remain fully available, so transparent signalling can be effected between any number of Interchange-connected attached PBXs.

6.2 Supported Services

The IiQ Gateway provides transparency for:

- Basic Call BTNR 188 [Ref. B.24] Sections 6 and 7.
- Supplementary Services BTNR 188 [Ref. B.24] Sections 8 - 26, 28-48 with the exception that service options that use Single Channel Working are not supported.
- BTNR 188 Section 27 applies to Traffic Channel maintenance services between adjacent DPNSS PBXs and is inappropriate for the intervening H.323 network.

6.3 Interworking Between DPNSS and H.323 Equipment

With some constraints caused by irreconcilable differences between the signalling models, the IiQ Gateway will interoperate the following Services between DPNSS and H.323 clients:

- DPNSS Facility
- EN-BLOC Call
- OVERLAP Call

- SIC Bearer capability mapping:
  - DPNSS to H.323
    The only DPNSS SIC allowed is 10 hex (64kbit/s PCM G.711 A-Law or analogue). This will become 3.1 kHz audio (information transfer capability) with G.711 A-Law (layer 1 protocol) on the H.323 side. Note that the presence of BSS-P or BSS-M will not affect the mapping.
  - H.323 to DPNSS
    Any valid H.323 bearer will become a SIC of 10 hex on the DPNSS side. Current default is to add a BSS-P to the outgoing ISRM.
- CLC Calling party category mapping
- OLI Calling party number mapping
- CLI Connected party number mapping

6.4 Proxy Support for Supplementary Services

Proxy support for supplementary services is useful on calls where transparent signalling cannot take place, i.e. on calls between DPNSS and H.323 clients.

The IiQ Gateway reacts to DPNSS supplementary service signalling to make the call behave (as closely as possible) as it would if placed between 2 DPNSS PBXs; by this means, it maximises the chance of the call being successful.

With some constraints caused by irreconcilable differences between the signalling models, the IiQ Gateway provides proxy support between DPNSS and H.323 clients for the services shown in the following table:

Service Description	Section	To DPNSS	From DPNSS
Alerting party number	6		✔
Call Forward - Immediate	11.1	✔	
Call Forward - On Busy	11.2	✔	
Call Forward - On No Reply	11.3	✔	
Diversion Validation	11		✔
Call Transfer (Connected party info)	13	✔	✔
Hold	12	✔	✔
Redirection	22	✔	
Series Call	23	✔	
Night Service	25	✔	
Centralised Operator	26	Partial	Partial
Calling Number Presentation Restriction	48		✔

Note: The number in the second column identifies the section number in the DPNSS [188] Issue 7 specification. The third and fourth columns indicate whether the proxy support applies to calls from H.323 to DPNSS, calls from DPNSS to H.323 or both.

7 SCN Clock Synchronisation

The IiQ Gateway is not specified to have its own very high resolution clock tied to the National Public Network frequency, nor is it specified to accept a Kilostream clock input. The IP Network works quite asynchronously from the TDM Circuit Switched Network so the IiQ Gateway is unable to derive a clock from its IP side.

PBXs may have other connections to Circuit Switched equipment; in particular DASS2, ISDN 30 or ISDN 30e inputs. If so, regulations require that they synchronise to those external connections or, failing that they must synchronise to PBXs that do have such connections. Failing that they may take a separate Kilostream clock feed or, lacking any of these, they will be able to supply an internal clock that is at least as accurate as that in the IiQ Gateway.

Incorrect clock synchronisation on the SCN side of the IiQ Gateway can cause severe problems with modem and fax quality, and lesser problems with voice quality. Calls may also be dropped.

The IiQ Gateway must always be synchronised to an SCN Port. It will synchronise to Port 1 if operational or to Port 2 (in product variants with 2 ports) if Port 1 is not operational or its signal is unstable.

In the event that neither SCN Port is capable of providing a signal from which the IiQ Gateway can derive ISDN synchronisation, then and only then will the IiQ Gateway use its internal clock as a source. However, it must be noted that as there is no incoming signal, there is no useful outgoing signalling capability either. At best, the IiQ Gateway should be sending Remote Alarm signals to both PRI Ports.

Where IiQ Gateway units and an IP Network are used to replace an existing Megastream network, the Network Synchronisation Plan will have to be revised so that NO PBX is trying to derive ISDN clock synchronisation from the IiQ Gateway unit connections. This is not a deficiency in the IiQ Gateway and will hold true for any IP Voice equipment lacking an independent kilostream clock feed.

The IiQ Gateway should not be connected through one E1 Port to each of two PBXs unless the PBXs are synchronised (i.e. have some common interconnect other than the IiQ Gateway). If both PBXs are functioning correctly, it would be possible to design a Synchronisation Plan in which the IiQ Gateway unit takes synchrony from one PBX and feeds it to the other; however, this falls down when the link to the master PBX fails. The IiQ Gateway cannot take the other PBX as its clock source since it has been set to take its cue from the IiQ Gateway. The IiQ Gateway can fall back to its own clock for very short term outages, but this does not have the accuracy required to act as the master source for the duration of the PBX failure.

8 SNMP Traps

The IiQ 2030 Series Gateway is configured to generate SNMP Traps for up to 8 destinations. SNMP traps have been divided into six groups as follows:

Port Errors

Layer 1 Alarms

Major Alarm

System Events

Reset Traps

Call Info Traps

Access to the MIBs which define the IiQ Gateway Traps may be accessed via links provided on the SNMP Configuration page when using the Gateway Management Interface. Using the Save As facility in the browser, these MIBs may be saved to allow the information to be compiled into the Network Management System (NMS).

8.1 Port Error Traps

Trap Code	Description
1	Layer 1 is operational
2	Layer 1 is non operational
20	Layer 2 is misconfigured
21	Layer 2 is operational
22	Layer 2 is non operational
30	Layer 3 is operational
31	Layer 3 is non operational
32	Layer 3 disabled
35	Alarm propagation on
36	Alarm propagation off
40	Loopback mode detected
41	Loopback mode cleared
42	Port impedance is set to 75 ohm
43	Port impedance is set to 120 ohm

8.2 Layer 1 Alarm Traps

Trap Code	Description
3	Layer 1 enabled
4	Layer 1 disabled
5	Layer 1 no signal
6	Layer 1 receiving AIS
7	Layer 1 lost sync
8	Layer 1 transmitting AIS
9	Layer 1 receiving RAI
10	Layer 1 has excessive errors
11	Layer 1 receiving RAI and E bits
12	Layer 1 transmitting no signal

8.3 Major Alarm Traps

Trap Code	Description
45	Port is non operational
46	Port has been commissioned
47	Port has been decommissioned

8.4 System Events Traps

Trap Code	Description
50	Fatal or watchdog error
51	Major alarms have been acknowledged
62	Media card fatal
70	Factory/Post is set to POST
71	Factory/Post is set to FACTORY
72	Management IP address change from craft port
73	Management subnet mask change from craft port
74	Management IP address change from webserver
75	Management subnet mask change from webserver
76	New software has been installed
77	New software has been activated by the webserver
78	New software has been activated by the Craft port
79	Webserver login detected
80	Webserver logout detected
81	Webserver login fail
82	System fully operational

Trap Code	Description
83	Default configurations have been applied
84	FTP'd Route ID table successfully configured
85	FTP'd Route ID table configuration failed
86	FTP'd route IP Address table successfully configured
87	FTP'd route IP Address table configuration failed
88	FTP'd Number Translation table successfully configured
89	FTP'd Number Translation table configuration failed
91	Failed to restore configuration

8.5 Reset Traps

Trap Code	Description
55	The unit has been reset
90	Unit reset after restoring configuration

8.6 Call Information Traps

Trap Code	Description
60	Voice call statistics

Note: These statistics are only presented for calls using a voice codec, not T.38 fax calls.

9 Craft Port Management

9.1 Craft Port Functionality & Operation

The Craft Port provides a secondary means of managing the IiQ Gateway. It is used for presentation of self test results and basic IP address parameter set-up, as described in section *2 Installation*, and also provides a means by which low level functions and diagnostics may be accessed during normal operation.

The Craft Port would normally only be used to set up a **New Management IP Address**, when the unit cannot be accessed using the web browser based Gateway Management Interface.

This section describes the menus and options available using the Craft Port.

Note:

All Craft Port facilities are available with the unit in normal operation but the functions are service affecting. It is strongly recommended that the IiQ Gateway unit is taken out of service before accessing these Craft Port facilities.

Convention used:

```
Text displayed by the Craft Port
Variable text
```

Access

The Craft Port may be accessed by a dumb terminal or terminal emulator on a PC using the serial cable supplied with the IiQ Gateway unit.

Communication settings: RS232, 9600baud, 8 bit, no parity, 1 stop bit.

9.2 Main Menu

```
                    (variant) Gateway
                    =================
          (C) Copyright 2003 Westell Ltd.
              Version  XXX-XX RX.X.X

System time : THU FEB 20 05:32:15 2003

[a] - Network Configuration
[b] - Software/Boot Configuration
[c} - Utilities
[d] - Motherboard Configuration
[e] - Diagnostic Testing
```

Note: Menu items [d] and [e] are only available under the guidance of Technical Support and item [d] is password protected.

9.3 Network Configuration Menu

```
[a] - Display Network Boot Settings
[b] - Set Management IP Address
[c] - Set Management Sub Net Mask
[d] - Set Default Gateway IP
[e] - Set Media Default Gateway IP
[f] - Set Media Gateway IP Address
[g] - Set Media Gateway Sub Net Mask
[h] - Show Current Management IP Settings
[i] - Reset all IPs to NULL
[J] - Go to Main Menu
```

Display Network Boot Settings

```
Next Boot IP Address : 100.10.11.100
Next Boot SubNet Mask : 255.255.0.0
Next Boot Default Gateway IP : Not Set
Next Boot Media IP : 100.10.11.001
Next Boot Media SubNet Mask : 255.255.0.0
Next Boot Media Gateway IP : 168.10.1.214
```

Set Management IP Address

```
IP Address (X.X.X.X) :
```

Set Management Sub Net mask

```
Sub Net Mask (X.X.X.X) :
```

Set Default Gateway IP

```
Default Gateway (X.X.X.X) :
```

Set Media Default Gateway IP

```
Media Default Gateway (X.X.X.X) :
```

Set Media Gateway IP Address

```
IP Address (X.X.X.X) :
```

Set Media Gateway Sub Net Mask

```
Sub Net Mask (X.X.X.X) :
```

Show Current Management IP Settings

```
Current Network IP : 100.10.11.100
Current SubNet Mask : 255.255.0.0
```

Go to Main Menu

Returns you to the **Main Menu**.

9.4 Software/Boot Configuration Menu

```
[a] - Display Current Boot Settings
[b] - Set Boot Image
[c] - Software Version Information
[d] - Go to Main Menu
```

Display Current Boot Settings

```
Image to be Booted: Upgraded
```

Set Boot Image

```
This will set the software to boot on next reboot.
Press 'D' for the default image
Press 'U' for the upgraded image
Press 'X' to return
```

Software Version Information

(Currently not functional)

Go to main Menu

Returns you to the **Main Menu**.

9.5 Utilities Menu

These utilities are intended to clear the unit's identify for example when redeploying in a new network. The MAC Address, Serial Number, Product Variant Information, Date and Time, Channel Licences Enabled and SCN Settings will not be lost.

```
[a] - Reset to Factory Defaults
[b] - Set the Real Time Clock
[c] - Reboot
[d] - Go to Main Menu
```

Reset to Factory Defaults

```
This will default your system to Factory Defaults.
Your configurations will be removed.
The unit WILL require a REBOOT
Are you sure you want to continue ? (Y/N) :
```

Set the Real Time Clock

```
Enter Time And Date (HH:MM:SS DD-MM-YYYY) :
```

Reboot

Reboots the IiQ Gateway.

Go to Main Menu

Returns you to the **Main Menu**.

10 Fault Determination

10.1 Introduction

This chapter on Troubleshooting has sections which cover:

- Power on problems.
- First level diagnosis of operational problems.
- Detailed specific diagnostic and corrective procedures.

These sections are written for a user attending a new or failed installation. Flow charts outline the initial diagnostic procedure and direct the reader to specific procedures for the recommended recovery action.

These sections also provide an indication of the level to which remote diagnosis may assist.

When performing an installation, cabling problems are common.

The section on Port Failure Alarms shows how to diagnose the majority of these, using the information shown on the status display.

10.2 Power-On Problems

When an IiQ Gateway is powered on, it performs a series of self-tests to ensure the hardware is functioning correctly. Normal operation of the module is resumed only if all tests are successful.

The four STATUS LEDs and the Power LED on the front panel indicate the progress of tests.

If nothing is displayed, follow the Power Supply diagnosis procedure.

10.3 Management Interface Problems

You will not be able to log in to the Gateway Management Interface if:

- the Gateway IP Address or Subnet Mask are incorrectly set;
- another User is logged into the Gateway Management Interface;
- the last User hasn't logged out correctly and the Non-use timeout has not expired;
- the Self Test has failed;
- access is attempted from a different LAN segment and the Default Gateway IP Address has not been set up in the IiQ Gateway unit; or
- a connection is made to the web server before the unit is fully operational. This may result in a delay in displaying the main screen and could also result in question marks appearing in the SCN Status. This can be resolved by refreshing the page.

10.4 Operational Problems

The figure below shows how to pinpoint a failing piece of equipment or cabling by deduction from local equipment and IiQ Gateway alarm relay indications, assuming that the IP network and its diagnostic information are outside the control of the local management system.

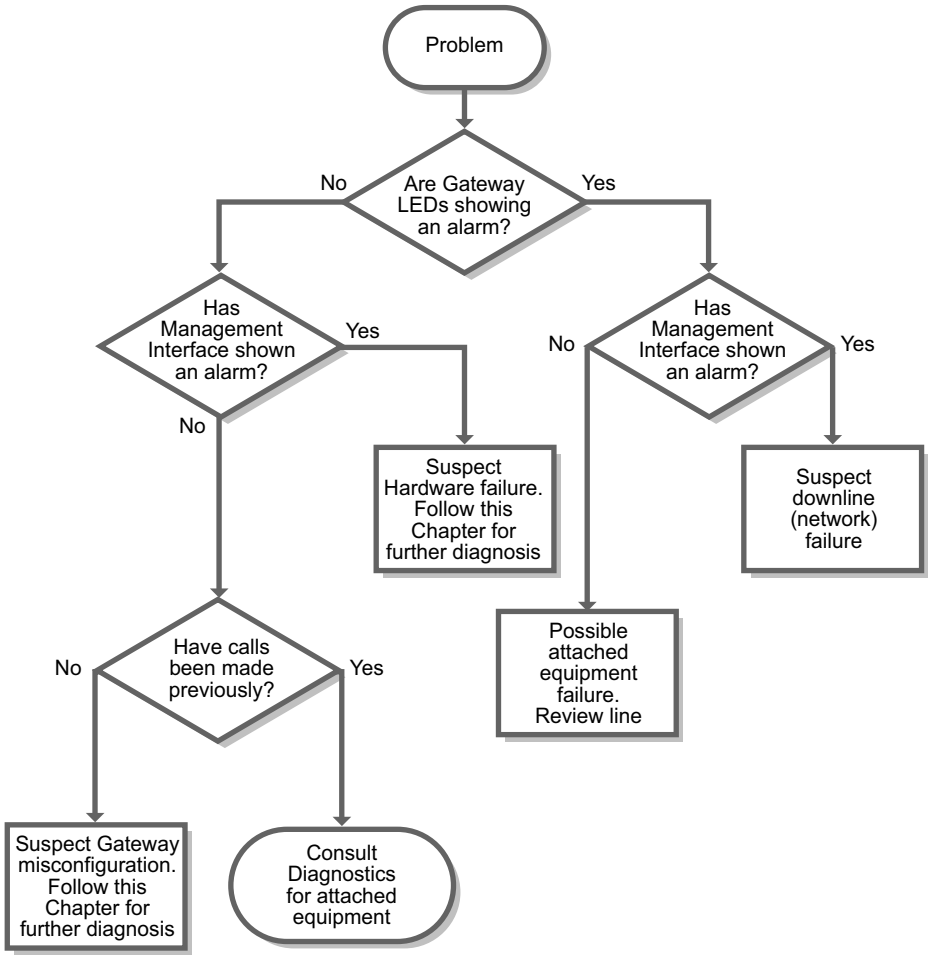


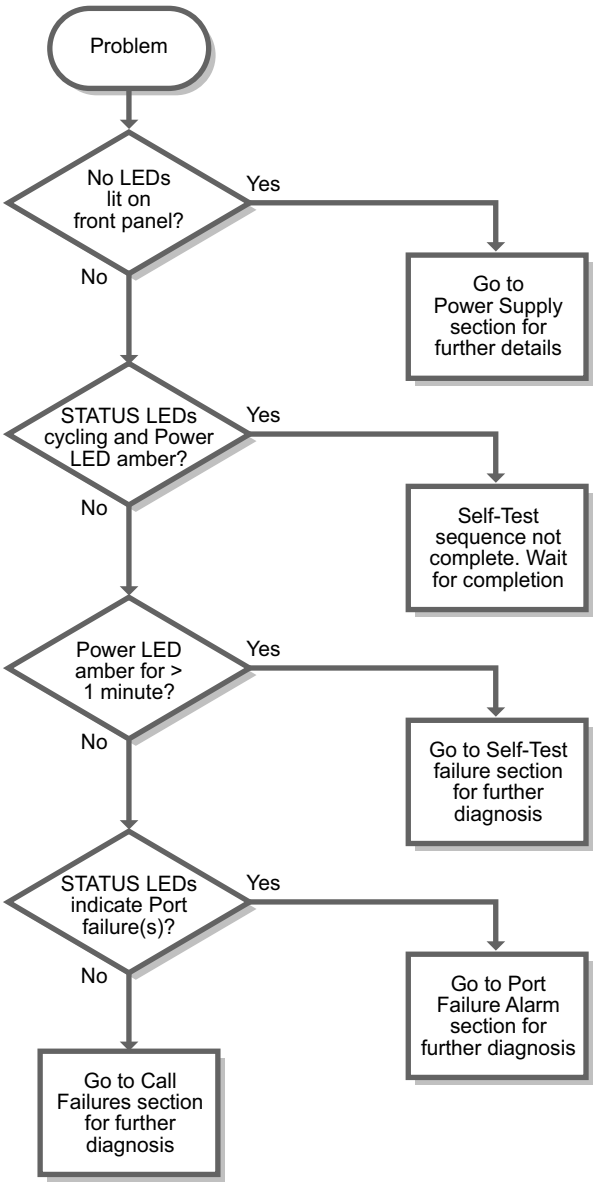
Figure: Problem Determination.

Problems are detected initially by one or a combination of the following symptoms:

- An alarm monitor detects that the alarm relay has triggered,
- A user advising of lack of service,
- An indication of Alarms from connected equipment, and or
- Error status on the LED display.

If a fault is indicated in the IiQ Gateway or the network beyond, you can interrogate for the status of each port if management terminal access is available. Otherwise, examine the status indications on the IiQ Gateway front panel.

Examine the status LEDs. In the normal operational state a LED is shown for each in-service port. If this is not the case, follow the checks outlined in figure below. This first level chart guides you to the most appropriate of the specific diagnostic procedures described in the Diagnostic Procedures section.



Problem Determination Check List.

10.5 Diagnostic Procedures

This section contains a set of diagnostic procedures which may be referenced directly or used in conjunction with the Operational Problems first level diagnosis flow charts.

Each procedure starts with a description of the symptoms of the error class, followed by a set of diagnostic actions which allows the actual fault to be pinpointed more accurately. Once this has been achieved it should be possible for the user to attempt to correct the fault.

10.5.1 Power Supply

Symptoms

No LEDs illuminated.

Diagnostic actions

1 Check there is power to the unit and the unit is switched on.

2 Check for fuse failure in the power feed or on the rear panel of the unit.

3 If still unable to locate the problem, the IiQ Gateway unit must be returned for repair.

10.5.2 Self Test Failure

Symptoms

The **Power** LED remains amber for more than one minute.

Diagnostic action

The hardware self-test has failed.

If the BNC cables (75Ω E1) are connected, power OFF the unit and disconnect the cables. Repeat the test and if the unit successfully completes self-test, the Tx and Rx cables are reversed.

Note: The unit will fail self test if the E1 ports are looped back to each other.

Power OFF and connect a dumb terminal (or PC with a terminal emulation program) to the Craft Port and set the Craft Switch to **CRAFT** Mode. Power ON to reset the unit. The IiQ Gateway will Self Test again and the terminal will display any failures. If there are no Self Test failures but the **Power** LED remains amber, check that the POST switch has not been left in the **Factory** setting. If it has, power **OFF** the unit, switch the POST switch to **POST** and power **ON** the unit. It should now pass and exit Self Test.

If the unit continues to fail the self test:

- Contact your second line support engineers for assistance, if needed.
- Return the failed unit for repair, with a note of the errors reported to the terminal.

Symptoms

The **Power** LED remains amber for more than one minute, the **S2** status LED is blinking and all other status LEDs are off.

Diagnostic action

Check if the Craft cable is attached to the unit but the other end of the cable is not attached to a dumb terminal (or PC with a terminal emulation program). If this is the case, power OFF the unit, disconnect the cable and then power ON the unit. It should now pass and exit Self Test.

Alternatively, the IP addresses and sub-net masks may not have been configured.

Power **OFF** and connect a dumb terminal (or PC with a terminal emulation program) to the Craft Port and set the Craft Switch to **CRAFT** Mode. Power **ON** to reset the unit. The IiQ Gateway will start Self-Test again and request the IP addresses and sub-net masks if they have not already been set. Once Power On Self-Test has run to completion, power cycle the Gateway unit.

10.5.3 Port Failure Alarm

Symptoms

When there is a Port Failure alarm, it is indicated by either P1 or P2 LEDs showing amber.

Note: If both P1 and P2 LEDs show amber at the same time, this indicates that there is an un-acknowledge major alarm in the major alarm log.

Cause

The cause conditions are indicated by the STATUS LEDs as follows:

Ports	S3	S2	S1	S0	
	On	On	On	On	Layer 1 is disabled
	On	On	Off	On	Loss of signal
	On	On	On	Off	Layer 1 error detected other than loss of signal, Alarm indication signal is not being sent
	On	Off	On	Off	Sending alarm indication signal
	On	On	Off	Off	Layer 3 is disabled
	On	Off	Off	Off	Layer 2 is misconfigured
	Off	Off	On	On	Port is in loopback

Table of Status LEDs

More detailed information may be obtained via the Management Interface.

10.5.4 Checking Cables

- Check for continuity of both the inner conductor and the screen.
- Check for short circuits between the inner conductor and the screen.
- Check for correct attachment of connectors to cables.
- Hold the cables firmly and move the connectors to and fro thoroughly, then re-check as above.
- Check that the cables are 75 Ω and not 50Ω - the centre pin diameter is different.
- Perform local checks and ensure fault symptoms do not vary between them. If they do, a cable fault is indicated.

10.5.5 Call Failures

Symptom

The status LEDs show no faults but no calls can be made. There may be no indication of failure from attached equipment.

Diagnostic action

You can monitor the IiQ Gateway's ports in turn using Primary Rate signalling and H.323 protocol analysers. Check that calls are being received into the equipment and are being passed on to the associated port. If not, and the cause is not obvious from inspection of the analyser diagnostics, contact your supplier's Helpdesk.

If the attached equipment is indicating a problem, it may be possible to diagnose the fault by referring to that equipment's fault finding documentation.

Check that the Routing Tables have not been misconfigured.

Note: A common mistake is to use the media IP address instead of the signalling/management IP address.

Symptom

Call is simplex (uni-directional) some or all of the time.

Diagnostic Action

Media has conflicting IP addresses or the same IP address has been used more than once. Check assigned IP addresses and correct.

Symptom

Calls are dropped unexpectedly while in progress.

Diagnostic action

A common cause is transient transmission problems on the network-side connections. If a PC is available use the facilities in the Web browser interface to check whether errors are occurring on either port.

Check any attached equipment.

Symptom

The Gateway fails to process calls for a short period and then recommences processing normally.

Diagnostic Action

The internal watchdog timer may have reset the system due to a Major Error. Using the Gateway Management Interface, check the error logs and contact your supplier's Helpdesk.

Symptom

Higher than expected levels of unsuccessful call attempts.

Diagnostic action

In a DPNSS environment some or all channels may be incorrectly configured at Layer 3 (set to X or to Y at both ends) causing failure to resolve channel contention correctly. Therefore, the configuration must be reviewed.

Symptom

DPNSS transparency is not achieved across an IP network.

Diagnostic action

Elements within the IP network may be failing to pass H.450.1 encoded transparency. Review routers and firewalls in the network.

Symptom

Poor voice or fax quality.

Diagnostic action

This is most likely due to an overloaded network, a faulty telephone or other equipment. Check and if necessary replace the equipment. If the IiQ Gateway is replacing an existing Megastream network, the clock may not be properly synchronised on the SCN side of the IiQ Gateway. Revise the Network Synchronisation plan so that no PBX is trying to derive ISDN clock synchronisation from the IiQ Gateway's connections. See section *7 SCN Clock Synchronisation*.

Symptom

The green **LAN Speed** LED flickers On and Off. Operation is unreliable.

Diagnostic action

The unit is unable to correctly detect between 10 Mb and 100 Mb ethernet operation or is unable to correctly sense whether a straight or crossover cable is in use. Check that the cable is of the correct specification, is undamaged and is fully inserted at both the IiQ Gateway unit and other end. Note that 100 Mb ethernet can be very sensitive to cabling issues. If the problem cannot be resolved, contact your supplier's Helpdesk.

Symptom

Up or Down indication for Layer 1 or Layer 2 appears to be incorrect (for example, the indication is different to that shown on the external equipment).

Diagnostic action

Disconnect all SCN lines, wait 30 seconds and re-connect.

Symptom

A call is set up but has no voice path (it is silent at both ends0.

Diagnostic action

Check that the equipment (IiQ gateway or other) at both ends of the call is configured to have at least one codec in common. This problem will be seen if one end is set to only support G.729 and the other is set for G.711.

10.5.6 Fatal Errors

Symptom

Unexpected restart; calls in progress may be lost but the unit recovers within a couple of minutes and on examination appears to be functioning normally.

Cause

The software has detected an error which it can not correct. The problem could be due to a catastrophic hardware malfunction or a fault in the software.

Any permanent hardware failure is discovered by the self test function and the unit will not be returned to service. If the fault was transient, the unit re-initialises, clears any calls which may have been left hanging, and resumes normal operation.

Once properly installed, configured and operational, Gateway units are extremely reliable. Software-detected errors are seldom and it is usually impossible to diagnose the causative factors. Unless due to a persistent hardware problem, full recovery within a couple of minutes is automatic, although calls in progress at the time of the failure will have been cleared.

Diagnostic action

The error is recorded in the unit's event log automatically. When the unit has restarted, record the content of the following Logs:

- System
- Port
- Major
- Port Error
- Call Statistics
- Call Signalling
- Codec Usage - Interval Statistics
- Codec Usage - Maximum Statistics

Contact your supplier for assistance.

10.6 Browser Interface Problems

Symptom

Unable to connect a Web browser to the Gateway Management Interface.

Potential cause and action

A user is already logged in to the IiQ Gateway or the last user has failed to log out. Retry connecting after waiting for the Non-Use Timeout period to expire.

Potential cause and action

Incorrect IP address entered. Type in the correct IP address. Confirm IP communications by 'pinging' the unit. If pings succeed, activity can be seen on the Ethernet Port LEDs. If the Non-Use Timeout has expired, access the unit using the Craft Port to confirm correct IP Addresses and Sub Net Masks. Reboot the IiQ Gateway and, if communication is restored, check the logs for errors.

Symptom

Management screens not updated as expected.

Potential causes and action

The Web browser has presented a cached page. The time and date information sent from the IiQ Gateway is recorded as earlier than the cached page date and time information, or the browser has been configured not to check for newer versions of stored pages.

Make sure that the browser is appropriately configured to check for newer versions of stored pages. Use the Web browser's 'delete all temporary files' or 'clear cache' facility and retry.

Symptom

A valid password is not accepted and no message appears stating that an incorrect password has been entered.

Potential cause and action

The Web browser is set to refuse cookies. Change the setting in the Web browser. If necessary, first consult your System Administrator.

Symptom

Management system menus absent and/or error messages about j/script support presented.

Potential cause and action

The Web browser is set to disallow javascript. Change the setting in the Web browser. If necessary, first consult your System Administrator.

Symptom

Window selected from menu will appear (probably with no content) and then disappear.

Potential cause and action

The browser has been set to disable pop-ups. The InterChange iQ Gateway requires that pop-ups be enabled in the browser for the management program to function correctly.

Appendix A Approvals, Safety Instructions & Statutory Information

This information must be read prior to use of this equipment and overrides as appropriate any information in respect of connection and use of the equipment.

Address any enquiries regarding regulatory aspects of this equipment to Westell Limited.

A.1 Connection to Mains Voltage Supply

The wires in the mains lead are coloured in accordance with the following code. As the colours of the wire in the mains lead may not correspond with the coloured markings in the plug, proceed as follows:

1 The wire coloured GREEN and YELLOW must be connected to the terminal marked E or by the earth symbol or coloured GREEN, or GREEN and YELLOW.

2 The wire coloured BLUE must be connected to the terminal marked N or coloured BLACK or BLUE.

3. The wire coloured BROWN must be connected to the terminal marked L or coloured RED or BROWN.

A.1.1 Replacing the mains fuse

Warning:

For continued protection against the risk of fire and shock hazard, replace fuses only with the same type and rating.

Fuse type: T2A H 250V.

A.2 Product Servicing

This product contains no user-serviceable parts. Any attempt by non-qualified personnel to gain access inside the product enclosure will compromise the terms of the approval quoted above. Should such access be attempted, liability will not be accepted if the equipment is shown subsequently not to be in compliance with the terms of approval.

Caution

To avoid electric shock, do not remove covers

Warning:

This equipment must only be installed and maintained by qualified service personnel.

A.3 Network Connections

This apparatus has been approved by the British Approvals Board for Telecommunication under Section 22 of the Telecommunication Act 1984 for connection to the following:

1 Private Circuits at interfaces in the UK compatible with G.703 (75 Ohms) at 2048 Kbits/s, or

2 Private Circuits at interfaces compatible with G.703 (120 Ohms) at 2048Kbits/s.

A.4 Equipment Port Classification

The ports are classified as follows:

Name	Type
Port 1	TNV1
Port 2	TNV1
Ethernet	SELV
Alarm	SELV
Craft	SELV

A.5 Safety Compliance

Safety complies with EN60950, IE C950, AS/NZS 3260, UL 1950.

A.6 EMC Compliance

EMC complies with EN55022, EN50082-1, AS/NZS 3548.

A.7 Protective Earth Cable

The units must be installed with a protective earth in accordance with EN 60950:2000 Clause 6.1.2.2. This requires a PVC covered earth cable (longitudinal Green and Yellow coloured stripes in accordance with EN 60950 / IEC 950) and must be connected to the chassis earth stud on the back of the unit.

The specification of the earth connecting cable is:

Current rating 17 Amps, with a cross sectional area of 1.5 mm^2, Wire 7/0.53 mm. Terminated at the IiQ 2030 Gateway unit with an M3 ring terminal 1-2.6 mm^2 conductor.

Note:

When the 75 Ohm BNC connectors are in use, permanent earthing replaces the requirements of clause 6.1.2 of EN 60950 as both the TNV and SELV circuits have an earth connection.

A.8 Lithium Cell

This product includes an Integrated Circuit which contains a Lithium Cell. This device is identified by the words Lithium Battery on its case and is fitted in position U4 on the processor card (M48T37V-10MH 1 TR).

The following warning should be strictly adhered to. Do not attempt to open this device.

Caution:

Risk of explosion if battery is replaced with incorrect type.

Dispose of used batteries according to instructions.

Do not dispose of in fire.

A.9 Flammability

Flammability meets the requirements of EN 60950, IEC950, and AS/NZS 3260.

A.10 Environmental

The InterChange iQ 2030 Series product meets the requirements of ETS 300 019-2-3 and IEC 68-2 for Shock and Vibration.

A.11 CE Mark

To meet the essential requirements of the R&TTE Directive (1999/5/EC), the following declarations are made for CE marking:

A.12 EMC Declaration of conformity

The InterChange iQ 2030 Series product meets the requirements of the European Electromagnetic Compatibility (EMC) Directive 89/336/EEC.

The product complies with the requirements of EN55022 (CISPR 22) Radiated and Conducted Emissions and EN50082-1 Electromagnetic Immunity for limits of radio disturbance characteristics of Information Technology Equipment (ITE).

Warning:

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Note:

The domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus concerned.

A.13 Safety Declaration of conformity

The InterChange iQ 2030 Series product meets the requirements of the European Low Voltage Directive (LVD) 73/23/EEC.

The product complies with the requirements of EN60950 for safety of information technology equipment, including electrical business equipment.

A.14 Special National Conditions

Norway

The local distributor of the InterChange iQ 2030 Series product in Norway must attach a self adhesive label placed just above the fuse rating, which is situated above the mains inlet filter. This label displays the following text in Norwegian:

Apparatet ma kun tilkoples jordet stikkontakt

Sweden

The local distributor of the InterChange iQ 2030 Series product in Sweden must attach a self adhesive label placed just above the fuse rating, which is situated above the mains inlet filter. This label displays the following text in Swedish:

Apparaten skall anslutas till jordat uttag nar den ansluts till ett natverk

Switzerland

The local distributor of the InterChange iQ 2030 Series product in Switzerland must supply a moulded plug that conforms to SEC/ASE 1011.

Denmark

The local distributor of the InterChange iQ 2030 Series product in Denmark must ensure that the power supply cord is provided with a moulded plug.

Appendix B References & Technical Specifications

B.1 References

[1] ITU G.703:1998 Series G: Transmission Systems and Media, Digital Systems and Networks - Physical / Electrical Characteristics of Hierarchical Digital Interfaces.

[2] ITU G.704:1998 Series G: Transmission Systems and Media, Digital Systems and Networks - Synchronous Frame Structures used at 1544, 6312, 2048 and 44 736 kbits/s Hierarchical Levels.

[3] (Safety, Europe) EN 60950:1992 Information processing and business equipment with amendments 1, 2, 3 and 4.

[4] (Safety, Europe) EN 41003:1996 Equipment to be connected to telecommunication networks.

[5] (Safety, Europe) ETS 300-046:1992 Parts 1, 2 and 3 ISDN primary rate: safety and protection.

[6] (Safety, International) IEC 950:1993 Information processing and business equipment with amendments 1, 2, 3 and 4.

[7] (Safety, Aust. and NZ) TS001:1997 / AS/NZS3260:1993 Information processing and business equipment, terminal equipment safety.

[8] (EMC, Europe) EN55022:1998 Radio frequency emissions, ITE / telecoms emissions.

[9] (EMC, Europe) EN50082-1:1997 Electromagnetic compatibility generic immunity standard for domestic, commercial and light industrial environments.

[10] (EMC, Europe) EN61000-3-2:1995, EN60555-2 LF Conducted emissions (harmonics).

[11] (EMC, Europe) EN61000-3-3:1995, EN 60555-3 Voltage fluctuations.

[12] (EMC, Europe) ETS 300 386:1994 EMC Requirements for Public Telecoms Network Equipment.

[13] (EMC, International) CISPR22:1997 Radio frequency emissions, ITE / telecom emissions.

[14] (EMC, Aust and NZ) AS/NZS 3548:1997 Limits and methods of measurement of radio interference characteristics of information technology equipment.

[15] (Environmental, Europe) ETS 300 019:1994, Part 2 Environmental conditions and environmental tests for telecommunications requirements.

[16] (Environmental, International) IEC-600 68-2 series, Basic environmental testing procedures.

[17] DPNSS [188] 2001 Digital Private Network Signalling System No.1 (DPNSS1).

B.2 Technical Specifications

B.2.1 Environmental

Ambient Temperature:	Operating: 0 C to +40 C. Storage: -10 C to +60 C.
Relative Humidity:	5% to 95% (non-condensing).
Safety:	Conformant with EN 60950 [3]; EN 41003 [4]; UL 1950; ETS 300-046 [5]; IEC 950 [6]; TS001/AS/NZS 3260 [7].
RFI Emissions (Class A):	Designed to meet EN 55022 [8]; EN 61000-3-2 [10]; EN 61000-3-3 [11]; ETS 300 386 [12]; CISPR22 [13]; AS/NZS 3548 [14].
RFI Immunity:	Designed to meet EN 50082-1 [9].

B.2.2 Physical

Height:	1U (44.45 mm).
Width:	439 mm.
Depth:	260 mm.
Chassis:	Plated pressed steel.
Front Panel:	Plated pressed steel with paint finish.
Weight:	1.4 kg.
Cooling	Side to side forced
Mounting	19” Rack mounting or free standing.

B.2.3 Reliability

MTBF:	> 30,000 hours.
MTTR:	30 minutes. There is no field repair option. The unit is replaced and returned for factory repair.

B.2.4 Real Time Clock/NVRAM Devices

This device is powered by a Lithium battery:

Predicted Operational Life:	> 20 years.
Predicted Storage Life:	1 year at 70° C, or 4.8 years at 30° C, worst case.
Clock Accuracy	± 1.6 Minutes per month at 25° C

B.2.5 Power

Operating Input Voltage Range:	100 to 230 VAC.
AC Frequency:	60 or 50 Hz.
Power Consumption:	Maximum 25 Watts.
Power Supply:	Integral Universal Input Power Supply Unit.

B.2.6 Primary Rate Interfaces

Primary Rate Interfaces:	2
Connectors:	RJ 45 (120 Ω) or BNC (75 Ω)
Line Interface:	CCITT G.703[3], 2.048Mbits/s, 120 Ω balanced or 75 Ω unbalanced.
Line Encoding	HDB3, clear channel capability.
Frame Structure	CCITT G.704 at 2.048Mbit/s [2]; CRC-4 multiframe mode.
Sub-equipped channel configurations	Fully configurable in DPNSS.
Frame loss & alignment	CCITT G.706 at 2.048Mbit/s.
Signalling Channel	TS 16 Common channel signalling timeslot 16.
Signalling Protocols	DPNSS: DPNSS [188] Issue 7 sections 1-6 plus some supplementary services; NFAS optional); QSIG: ETS 300 172 (1995).
Signalling Orientation	All protocols fully ET/PBX configurable.

B.2.7 Clocking

Clock Source:	The unit can be synchronised to either primary port. The Gateway will synchronise to SCN Port 1 if working or SCN Port 2, if Port 1 is not available or is supplying an unstable signal.
Internal Clock Stability:	E1 - 2.048Mbit/s ± 100 ppm.

B.2.8 Codecs Supported

G.711 A-law, G.711 μ-law, G.729A

B.2.9 Management Interface

Web Browser	Microsoft IE 5.0 or later. Netscape 6.0 or later.

Appendix C Connectors & Cabling

C.1 Ethernet Port - 100Mbs

Connector		RJ45.
	Pin 1:	TxD+.
	Pin 2:	TxD-.
	Pin 3:	RxD+.
	Pin 6:	RxD-

C.2 Alarm Port

Connector		Weidmüller BL5.08 Orange 3 way connector with terminal screws.
	Pin 1:	Normally Open (NO) (left pin when looking at the rear panel).
	Pin 2:	Common.
	Pin 3:	Normally Closed (NC).
Maximum voltage/ current		60V at 500mA over the operating ambient temperature range.

C.3 Craft Port - Craft Mode

V.24/V.28 (RS232).

Connector:		9 pin, female D type.
	Pin 2:	TxD
	Pin 3:	RxD
	Pin 5:	GND
Modem Control:		None.
Flow Control:		None.
Speed:		9600 bit/s.
Characteristics:		8 bits, no parity, asynchronous, 1 stop bit.
Configuration:		Interactive ASCII menu text interface.
Management Protocol:		Structured ASCII command/response interface.

Craft Port - Factory Mode

V.24/V.28 (RS232).

Connector:		9 pin, female D type.
	Pin 2:	RxD
	Pin 3:	TxD
	Pin 5:	GND
Modem Control:		None.
Flow Control:		XON/XOFF.
Speed:		38400 bit/s.
Characteristics:		8 bits, no parity, asynchronous, 1 stop bit.
Configuration:		Interactive ASCII menu text interface.
Management Protocol:		Structured ASCII command/response interface.

Appendix D Glossary of Terms

This is a Glossary of Terms and Acronyms used throughout this document.

Word/ Phrase/ Acronym	Meaning
A	
ADPCM	Adaptive Differential Pulse-Code modulation
AIS	Alarm Indication Signal. A signalling condition of all '1's on a Primary Rate interface, indicating that the PRI equipment has failed.
ASCII	American Standard Code for Information Interchange.
B	
BTNR	British Telecommunications Network Requirement.
C	
CELP	Code Excited Linear Prediction.
CLC	Calling/Called Line Category.
CLI	Calling Line Identifier.
codec	Coder Decoder.
D	
DASS2	Digital Access Signalling System Number 2. The current version of the DASS protocol. Often just referred to as DASS.
DiffServ	Differentiated Services
DPNSS	Digital Private Network Signalling System.
DTMF	Dual tone multi-frequency.
E	
ECP	Encryption Control Protocol.
Ethernet	Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation.
ETSI	European Telecommunications Standards Institute.
F	
Fast Start	Part of the H.248 / H.323 standards. Fast Start reduces voice path connection delay during call setup.
G	
G.711	Describes the 64 Kbit/s PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs. This is described in the ITU-T G-series recommendations.
G.723	Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards.

G.729a	Describes CELP compression where voice is coded into 8 Kbit/s streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32Kbit/s ADPCM and are described in the ITU-T standard in its G-series recommendations.

H

H.225	An ITU standard that governs H.225.0 session establishment and packetisation. H.225.0 actually describes several different protocols: RAS, use of Q.931 and use of RTP.
H.245	An ITU standard that governs H.245 endpoint control.
H.323	Extension of ITU-T standard H.320 that enables videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.
H.450	An ITU standard that defines supplementary services
Hz	Hertz.

I

IP	Internet Protocol.
ISDN	Integrated Services Digital Network.
ITU	International Telecommunication Union.
ITU-T	Telecommunication standardization sector of ITU.

L

LAN	Local Area Network.
LED	Light Emitting Diode.

M

MCU	Multipoint Control Unit.
MIB	Management Information Base.

N

NFAS	Non-Facility Associated Signalling.
NMS	Network Management System.
NTP	Network Time Protocol.
NVRAM	Non-Volatile Random Access Memory.

O

OLI	Originating Line Indicator (ITU-T/CCS #7).

P

PAP	Password Authentication Protocol.
PAMS	Perceptual Analysis Measurement System.
PHB	Per-Hop Behaviour.
PBX	Private Branch eXchange.
PC	Personal Computer.
POST	Power On Self Test.

Prepend	Add to the start of.
PRI	Primary Rate Interface.
PSQM	Perceptual Speech Quality Measurement.
PSTN	Public Switched Telephone Network.

Q

Q.931	ITU-T specification for signalling to establish, maintain, and clear ISDN network connections.
QSIG	A signalling standard. Common channel signalling protocol based on ISDN Q.931 standards and used by many digital PBXs. Q (point of the ISDN model) Signalling.
QOS	Quality of Service.

R

RADIUS	Remote Authentication Dial In User Service (RFC 2865).
RAI	Remote Alarm Indication. An indication in the channel framing information on a Primary Rate Interface showing that the equipment signalling the condition detects a problem in the link or attached equipment.
RAS	Registration Admission and Status
RS-232	Recommended Standard 232 (computer serial interface, IEEE).
RTCP	Real Time Control Protocol (RFC 1889).

S

SCN	Switched Circuit Network.
SIC	Service Indicator Code.
SNMP	Simple Network Management Protocol.

T

T.302	Part of the H.248 / H.323 controls standard.
TCP	Transmission Control Protocol.
TDM	Time Division Multiplex.
ToS	Type of Service.
TS	Time Slot.

U

UDP	User Datagram Protocol.

V

VAD	Voice Active Detector.
VPN	Virtual Private Network.

Appendix E Useful Information

E.1 Echo Cancellation

Echo problems in telephony arise from a variety of sources. However, the effect to a user is consistent; what is said into the handset is echoed by the system after a short delay. The presence of echo may be masked or exacerbated by different network effects, most typically by network delay, as this can in effect insert a gap during which echo can be discerned, where otherwise it would be masked by conversation.

Individual perception is also important; some people are more sensitive to echo than others. Audio acuity plays an important part as echo is almost invariably quieter than the general level of conversation in a call. A total absence of echo in a system is disconcerting to a user, as the human ear expects a degree of feedback. Echoes of a certain volume/delay can render speech almost impossible. In practice, from a users perspective, echoes occurring before 45 to 50 ms are unobtrusive. Those occurring after 128 ms are unusual.

Echo is a 'far end' problem in telephony systems. Issues at the receiving end cause problems, rather than analogous issues at the transmitting end which occur too quickly to be perceived as echo. Major causes of echo are the 2-4 wire conversion (typically in the PBX) and acoustic feedback at the handset.

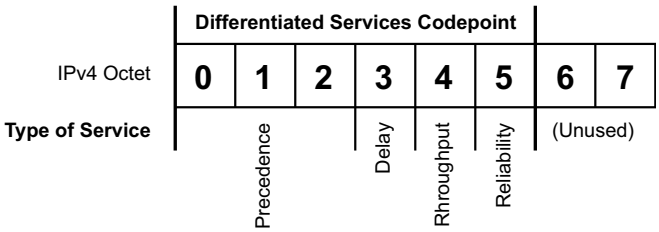
In order to detect echo, the voice packetization section of an IiQ Gateway adopts a style of 'near end' echo cancellation. Perversely, this means that echo cancellation is done at the far end of a call *nearest* to the source of the echo (thus 'near end', in this context, is relative to the source of the echo). This avoids additional complications caused by the echo transiting the network and being subject to further delay, jitter, etc. In comparing system capabilities, and determining appropriate configuration parameters, care must be taken to distinguish between the echo cancellation periods appropriate for 'near end' cancellation and the longer ones required for the alternative 'far end' cancellation.

In order to detect echo, a comparison between transmitted and received data is made, and echoes detected removed. This is achieved without clipping genuine received data. Obviously the longer this comparison period is, the more computational power is required and the more complex things become. To avoid comparing over a long period, at the start of a call the path delay for potential echoes is determined, and then a user configurable period of echo cancellation of up to 32 ms is applied (thus cancellation is applied only during the period when echoes are likely to occur).

In a typical trunk replacement application, where a pair of IiQ Gateways are used in place of an E1 link between PBXs, echo cancellation in the gateway may be superfluous if the function is carried out by the PBXs. However, it should be turned on in the gateway unless the user has confirmed that it is not required, in both theory and practice.

E.2 Quality of Service

The IiQ2030 Series Gateway permits Quality of Service to be specified for IP packets for both Media and Call Signalling. This can be configured either by using **Type of Service** settings or **Differentiated Services Codepoints,** as required by the host IP network. The **Differentiated Services Codepoint** uses the same fields in the IPv4 Octet as in **Type of Service** Precedence, Delay, Throughput and Reliability.



These six bits in the IP header field are set to determine how packets are forwarded by the nodes inside the network, and to condition the marked packets at network boundaries in accordance with the requirements of each service.

The **Differentiated Services Codepoint** is mapped to the Per-Hop Behaviour (PHB) that defines how a packet is handled at each node of the network. Nodes may be set to rewrite the codepoint as needed to provide a desired local or end-to-end service.

Increasing the performance of one of the Quality of Service parameters is most likely to be at the expense of another and therefore settings should only be changed under the control of or with instructions from the Network Administrator.

Codepoint 000000 defines use of the default PHB for the Internet; its behaviour is fixed.

The default **Quality of Service** settings for the IiQ 2030 Gateway are:

Differentiated Services Codepoints

Media	000000
Call Signalling	000000

Type of Service

Media	Precedence	0
	Delay	Normal
	Throughput	Normal
	Reliability	Normal
Call Signalling	Precedence	0
	Delay	Normal
	Throughput	Normal
	Reliability	Normal

E.3 Using with GPT / Siemens Equipment

When using the IiQ Gateway with GPT / Siemens Realitis DX or iSDX, **D Channel Link Tests** on the PBX must be switched off. This is done by using the **RTCT** command. See the appropriate manufacturer's User Manual for further information.

E.4 Maintenance Replacement

In the unlikely event that an IiQ Gateway should fail, it may be necessary to replace it with a maintenance spare which will need to be configured to the same settings as the field IiQ Gateway. This is best achived by restoring a configuration back up file. Cofiguration back up files are software version specific and to restore the configuration of the failed IiQ Gateway unit to the replacement unit, the replacement unit must first be loaded with the same software version as the failed unit.

If the replacement IiQ Gateway is at a different software level, the applicable software must first be downloaded to it and then the restore performed. The software in the replacement unit can then be upgraded. If this new software version is already pre-loaded in the replacement Gateway as its default software, upgrade is achieved by re-activating the default sofware. Otherwise, new software must be downloaded. When the upgrade is completed, a new configuration back up should be saved.

E.5 Hop Counts (Time to Live)

E5.1 Ping

The IiQ Gateway may ping from both the management/signalling IP address and the media IP address. However, the handling of the ping requests differ between these addresses as follows:

- A ping request from the management/signalling IP address has a hop count of 64
- A ping response from the management/signalling IP address has a hop count of 64 or the hop count from the ping request, whichever is greater.
- A ping request from the media IP address has a hop count of 20
- A ping response from the media IP address uses the hop count from the ping request.

For example, with a ping request between two units taking 9 hops from one to the other, a ping request from the management/signalling IP address on one unit to the management/signalling IP address on the other would be issued with a hop count of 64 and recieved by the destination unit with a hop count of 55. The ping response to this request would be issued with a hop count of 64 and recieved by the original unit with a hop count of 55. A ping request from the media IP address on one unit to the media IP address on the other would be issued with a hop count of 20 and recieved by the destination unit with a hop count of 11. The ping response to this request would be issued with a hop count of 11 and recieved by the original unit with a hop count of 2.

E5.2 Other Packets

All other packets, whether generated by the management/signalling IP address or the media IP address have a hop count of 64.

Westell Limited
Ringway House
Bell Road
Daneshill
Basingstoke
Hampshire, RG24 8FB
United Kingdom

Tel: +44 (0) 1256 843311
Fax: +44 (0) 1256 840429
Help Line: +44 (0) 1256 842285
email: info@westell.co.uk
Website: www.westell.co.uk