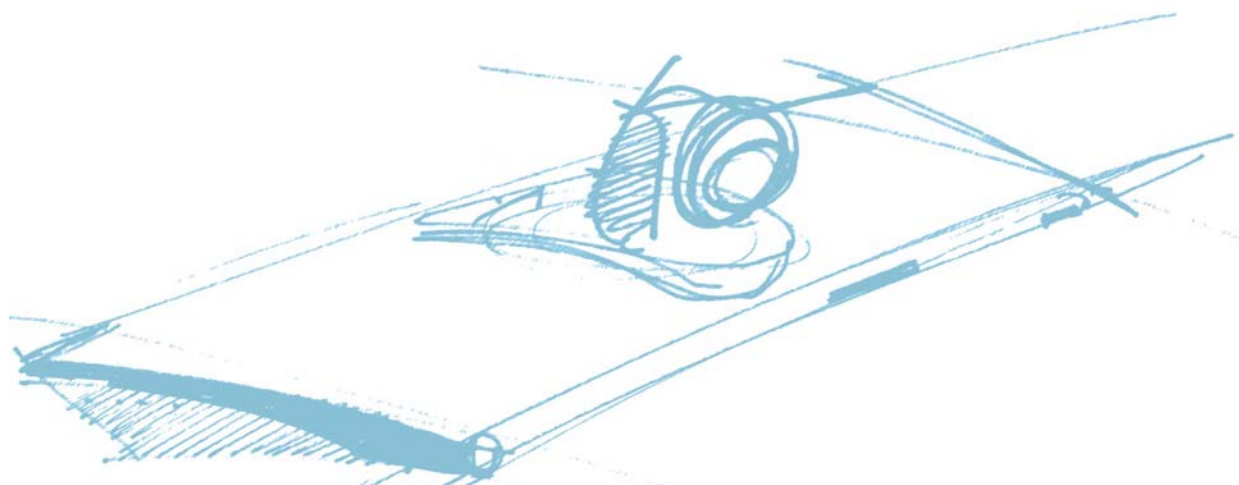


Vega X3

Use and Installation Manual

Welcome

















Thank you for choosing a AETHRA® SpA. Product.
Inside you will find useful information to help you get the most out of the Aethra product.
The information contained in this manual is subject to change without prior notice
by Aethra SpA.

INDEX




SAFETY RULES	5
ABOUT THIS MANUAL	6
ABOUT VEGA X3 SYSTEM	7
PRELIMINARY	7
GENERAL INTRODUCTION	7
FEATURES AT A GLANCE	7
VEGA X3 SYSTEM COMPONENTS.....	7
REMOTE CONTROL	8
CABLING SCHEME	11
VIDEOCONFERENCE TIPS	12
SYSTEM POSITIONING AND INSTALLATION	13
CONNECTING THE AETHRA POD	14
OPERATION AND USE	15
FIRST TIME EQUIPMENT IS SWITCHED ON	15
MENU STRUCTURE	16
HOW TO MAKE A CALL	18
HOW TO MAKE A CALL FROM PHONEBOOK	18
AUDIO-VIDEO CALLS	19
TO RESELECT AN INCOMING OR OUTGOING CALL	20
TCS-4 MODE VIDEO CALL	20
AUDIO CALL	20
SECURE CONNECTIONS	20
HOW TO RECEIVE A CALL	21
DUAL VIDEO MODE	21
<i>Dual Video Connection</i>	21
<i>Dual Video Disconnection</i>	22
USING THE PHONEBOOK	22
<i>Entering Names in the Phonebook</i>	22
<i>Modifying and Erasing Phonebook Entries</i>	23
<i>Connecting to a global Remote Phonebook</i>	23
VIDEO INPUT MANAGEMENT	24
VIDEO PRIVACY	24
CONTROLLING AUDIO	25
VIDEO CAMERA PRESETS	25
SYSTEM CONFIGURATION - SETTINGS	26
USER PREFERENCES	26
<i>Control panel</i>	26
Display	26
Screensaver	26
Remote control	27
<i>Call-Answer-Mode</i>	27
General	27
H.320	28
Broadcast	28
<i>Display Status Bar and Transparency</i>	28
<i>Customize colors</i>	28
AUDIO – VIDEO – DATA	29
<i>Audio</i>	29
Inputs	29
Processing	30
Outputs	30
<i>Video Quality</i>	30
<i>Cameras</i>	30

Settings	30
Customize	30
Driver	31
<i>Monitors</i>	31
Settings	31
PiP-PaP	32
Plasma	33
<i>Data Channels</i>	38
INSTALLATION	39
<i>Password</i>	39
<i>Encryption</i>	39
<i>Licenses</i>	40
<i>Terminal Settings</i>	41
<i>Network interface</i>	41
ISDN network interface	42
Access Configuration (ISDN BRI Euro)	42
Access configuration (ISDN BRI National)	43
<i>IP configuration</i>	43
IP Configuration	44
H323 Settings	45
SIP Settings	46
Services	46
PPPoE	50
<i>Enable network</i>	50
LOCATION	51
<i>Load default settings</i>	51
PRESENTATIONS	52
Go back to previous slide	52
Go to next slide	52
<i>Slides storage</i>	53
<i>Slides recall via WEB client</i>	53
<i>Saving slides on a PC</i>	53
SYSTEM DIAGNOSTICS	53
<i>Terminal test</i>	53
<i>Interfaces</i>	54
<i>Connection Status</i>	54
<i>Hardware</i>	54
<i>Software Versions</i>	54
CONNECTING A PERSONAL COMPUTER	55
CONNECTING A PC TO THE SYSTEM WITHOUT LAN	55
CONNECTING TO THE SYSTEM VIA A PC IN A LAN	55
REMOTE MANAGEMENT	56
ACCESS TO THE WEB PAGE	56
UPDATING SOFTWARE	57
DATA CONFERENCE WITH MICROSOFT NETMEETING 3.XX	58
DOWNLOAD DATA CONFERENCE	58
<i>Managing the DataConference software</i>	59
APPENDICES	60
NETWORK REQUIREMENTS IP\H.323	60
NAT – FIREWALL INTEROPERABILITY	60
TECHNICAL SPECIFICS	64
TROUBLESHOOTING PROBLEMS	65
GLOSSARY	66
USE AND STORAGE CONDITIONS	67




SAFETY RULES

	DEVICE IN CLASS I Always connect to a grounded socket.
	To guarantee continuous protection for operator safety, only use the mains adapter supplied with the device.
	WARNING: for power supply connection use an easily accessible outlet located near the device. Never remove the mains plug for permanent connection.
	Connect the ISDN port to a network termination only (NT1). It is absolutely forbidden to connect the system to an outdoor telecommunication line.
	Connect the LAN port to an internal LAN circuit only. It is absolutely forbidden to connect the system to an outdoor telecommunication line.
	This equipment will be inoperable when mains power fails
	To guarantee continuous protection for operator safety, make sure that the Network interface is always inserted . If the Network Interface is not in place, do not under any circumstances remove the cover.
	The change from cold to hot environments can cause the formation of condensate inside the device. To avoid malfunctioning, wait at least 2hours before connecting the device to the supply mains.
	In case of fire, absolutely avoid using water to extinguish it.
	WARNING: RISK OF ELECTRIC SHOCK The power supply used by this device involves lethal voltage levels.
	Do not access internal parts of the device (and/or of the power supply unit).
	If objects or liquids penetrate inside the device, immediately disconnect the power supply cable. Before using the device again, have it checked by specialized staff.
	Refer to qualified staff for service.
	In case of intervention, always check that the power supply has been completely and successfully disconnected.





REGIONAL REQUIREMENT

	Laitte on liitettävä suojamaadoituskoskettimilla varustettuun pistorasiaan.
	Apparatet må tilkoples jordet stikkontakt.
	Apparaten skall anslutas till jordat uttag.


ENVIRONMENTAL WARD

	CAUTION: risk of explosion if batteries are replaced by an incorrect type. Dispose of used batteries according to the instructions.
	The batteries of this equipment must be recycled by a company in charge of this activity, a company qualified for the disposal of dangerous materials or by using containers provided for the separate collection of worn out batteries.
	This equipment may not be treated as household waste. Instead it shall be handed over to the applicable collection point for the recycling of electrical and electronic equipment. By ensuring this product is disposed of correctly, you will help prevent potential negative consequences for the environment and human health, which could otherwise be caused by inappropriate waste handling of this product. For more detailed information about recycling of this product, please contact your local city office, your household waste disposal or the dealer where you purchased this product.


WARNINGS

	CAUTION: many of the components used in this device are sensitive to electrostatic charge.
	In case of manipulation of the connection cables, disconnect the power supply and avoid direct contacts with the connector terminals.
	When handling electronic components, to eliminate any static electricity touch a grounded surface. If possible, wear a grounding arm band.
	Failure to comply with these warnings could cause permanent damage to device.


CLEANING

	To clean the device use a soft cloth either dry or moistened with a little detergent. Never use any type of solvents, such as alcohol or gasoline, to avoid damaging the finish.
---	--

EN55022 Classe A COMPLIANCE


	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.
---	--

FCC15 Classe A COMPLIANCE

	This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
---	---

About this manual

Used symbols and syntax

	Symbol related information must be followed very carefully
---	---

1. Instructions in a enumerated list must be accomplished following the reported order
2. order

NOTE Associated instructions give useful information

“Name” Name refers to particular hardware or software function

Remote control

Remote control controls all system functions (see “Remote control” chapter)

Remote control uses two 1.5V AAA alkaline batteries, and an alert appears on the status bar when batteries are low; user can change the batteries opening the cover on the remote control rear.

Insertion of the characters in the alphanumeric fields



For numbers or letters insertion it is possible to use the alphanumeric keyboard of the remote control or, alternatively, the virtual keyboard by pressing the “OK” key once positioned on the alphanumeric field.

Select the “Esc” key in the virtual keyboard to close it.

Main functions of the system can be performed using:

- icons in the graphical user interface.
- remote control keys

In configuration menus, these icons will always appear:

	Back to previous page
	Back to Home Page.

About Vega X3 system

Preliminary

The complete functionality and all associated configurations that are described in this manual, even if they are not included in the series production, are supported by the system as long as they are appropriately licensed.

General introduction

Vega[®] X3 is a high-performance system at the cutting-edge of set-top technology. It is ideal for small or medium group of people in a videoconferencing sessions that require enhanced audio and video quality. Easy to use thanks to the user friendly GUI managed by the new “one-touch” remote control.

Supports Multiple Connectivity

Available in several versions: for connections up to 128 kbps over ISDN BRI and 2 Mbps over IP; both for H.323 or SIP networks.

Simultaneous Dual-Stream Video

Convenient VGA/DVI-I input and output ports provide one-step PC plug-in for simultaneous dual-stream video and live PC presentations with enhanced images.

Customizable Graphic User Interface

The user is able to choose layouts and colours from a variety of alternatives.

Features at a Glance

- VGA/DVI-I input and output ports
- Dual-stream video.
- Support for two monitors.
- Supports ISDN, IP-H323,IP-SIP.
- Embedded PowerPoint[®] presentations.
- Supports AMX[™] and Crestron[™] protocols for keyboards and control panels.
- T.120 for multimedia.
- Full-duplex audio with echo cancellation.
- Automatic Noise Suppression.
- Remote diagnostics and management.
- Wireless LAN support.
- Web streaming function.

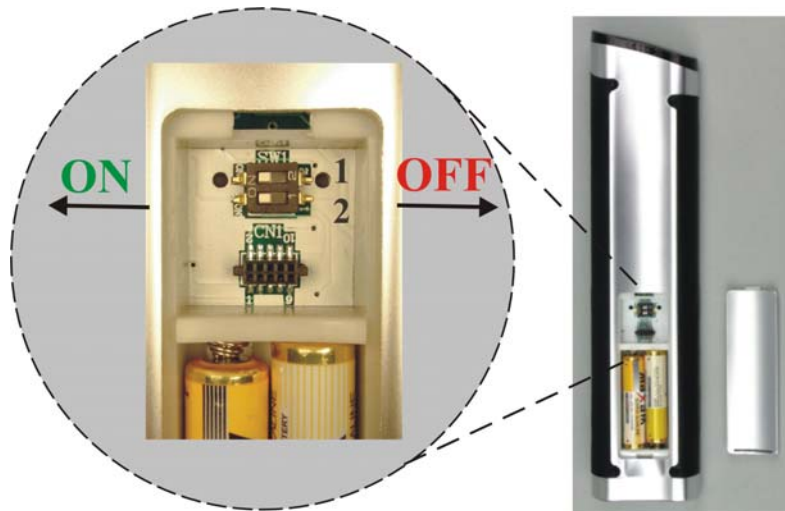
VEGA X3 system components

Main components of the VEGA X3 are:








- H.320/H323 Codec.
- Integrated Camera
- Aethra Microphone MiniPOD.
- Power supply whit cable.
- Infrared remote control.
- User manual.
- Monitor cables.
- DVI-I/XGA adapter
- SCART adapter
- PC serial cable adapter.
- RJ45-RJ45 cables.
- Packaging.

Remote control

Note In order to avoid un-desired controls reaching other systems, user can modify transmission power from 2mt to 20mt (default) by means of a switch in the battery space:
 Move both the Switches to **-ON** position → 20mt
 Move both the Switches to **-OFF** (1,2) position → 2mt



Remote control keys:

Key	Description function
	<p>“ON/OFF” Key It turns on and off the system. It puts the system in “screen saver” mode. It restarts the system from the “screen saver” mode. By pressing the key results in opening a window of notice:</p> <ul style="list-style-type: none"> • YES. Turn off the system. • NO. To enter “screen saver” mode.
	<p>“SEND” Key It sends slides/still pictures</p>
	<p>“SLIDE” Key Opens the integrated PPT presentation.</p>
	<p>“FAR/NEAR” Key Select the remote o local camera for PTZ.</p>
	<p>“DUAL” Key</p> <ul style="list-style-type: none"> • Once in connection, it activates the DualVideo functionality: the system asks for the second video source. • By pressing again the same key is possible to stop the DualVideo, without disconnecting the call.
	<p>“PiP” Key</p> <ul style="list-style-type: none"> • Activates/deactivates PiP (left upper corner being the PiP default position). • If enabled, moves the PiP (See “Control panel” paragraph).
	<p>“PRIVACY” Key</p> <ul style="list-style-type: none"> • Once in connection the system does no send any more video live but the customizable video privacy image.

- Not in connection activates/deactivates:
 - **Video privacy.** As above
 - **Don't disturb.** System does not answer to incoming calls (busy for the remote)



“Back” Key
Comes back to the previous interface page, without storing any parameter eventually modified.



“HOME” Key
Comes back to the Home interface page, saving any parameter eventually modified.



“SELF” Key
Activates/deactivates selfview.



“Help” Key
Activates/deactivates on line help.



“(- / +)” Keys

- ” **ZOOM**”: sets the camera zoom.



“Auto” Key

- Activates/deactivates the autotracking function.

“(- / +)” Keys

- “**VOL**”: sets the audio level.

“Mute” Key

- Activates/deactivates audio transmission.



“Arrow Keys”:

- allow navigation inside interface pages and camera movements.

“OK” Key:

- confirms actual selection.



“Call” Key:

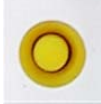
- Allows to call or receive an incoming call.

“Disconnect” Key:

- Disconnects a call.

“Phonebook” Key:

- Opens the phonebook.



“Function” Keys

- Red. Camera choice shortcut.
- Yellow. Camera choice shortcut.
- Blue. H.243 function shortcut.
- Green. Received slides/still images visualization shortcut.



“C-DEL” Key
Deletes characters



“CAMERA” Key

- Selects a video input.
- Usable as camera choice shortcut.

(see **Audio-Video-Data chapter, customize cameras**)



“MEMO-PRESET” Key
Saves the camera presets.



“SEL-PRESET” Key
Selects the camera presets.

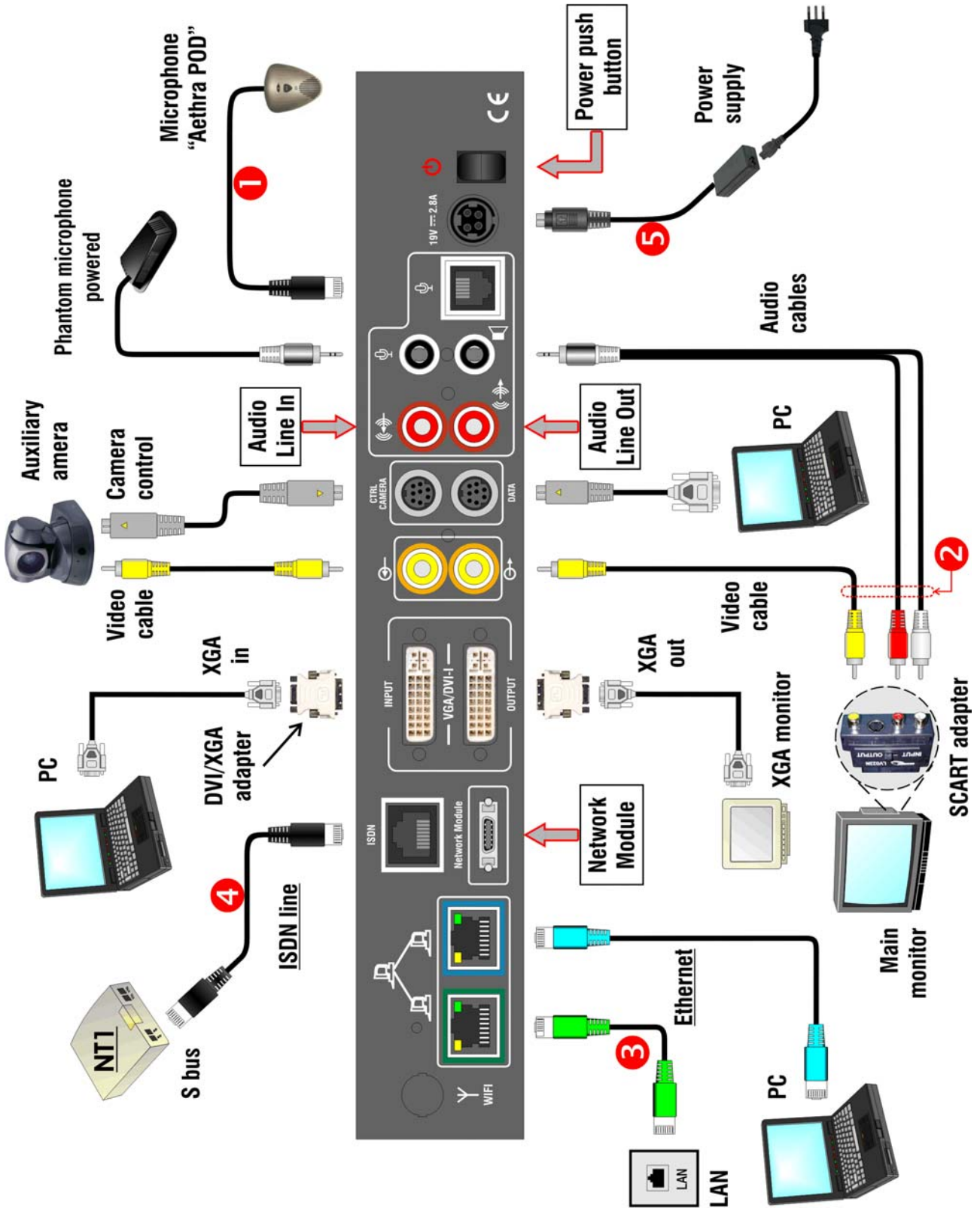


“Alphanumeric” Keys
It allows letters and numbers insertion.
“See the chart”

Remote control alfa-numeric symbols to keys association

KEY	SYMBOLS						
1	1	a	b				
2	2	c	d				
3	3	e	f	g			
4	4	h	i	j			
5	5	k	l	m			
6	6	n	o				
7	7	p	q	r			
8	8	s	t				
9	9	u	v	w			
0	0	x	y	z			
*	.	*	@		=	-	+
#	#	&	:	/	\		

Cabling Scheme



Videoconference tips

Tips to improve a virtual meeting, to optimize audio-video transmission and reception, and to fully enjoy all videoconference benefits.

Optimal Meetings

- Before starting a videoconference be sure that all you need is ready: addresses or numbers to call, lightning, microphones.
- Connect and test all peripherals eventually needed (document camera, VCR, PC/Laptop)
- Use natural gestures as in a real meeting
- Speak in your normal voice

Optimal Video

- Avoid contemporaneous usage of natural (changing) and artificial lightning
- Avoid direct artificial lightning
- Avoid “mobile” backgrounds (curtains moved by the wind)
- Try to fill the screen as much as possible with persons, not backgrounds

Optimal Audio

- Place the microphone on the table in front of people (use 2 microphones in case of big tables)
- Do not place papers or other objects in front of the microphone
- Don't rustle papers or tap on the table or microphone
- Mute the microphone before moving it.
- Speak in your normal voice

System positioning and installation



All operations should be carried out without connection to main power supply.
Connection to main power supply should only be performed after complete parts assembly.

Place the System in the desired location, and connect the follow equipments:

- 1) Connect the “Aethra POD” Microphone. (See cabling scheme, cable 1)
- 2) Connect System Audio/Video Outputs to main monitor (See cabling scheme, cable 2).
- 3) Connect the optional XGA monitor using the DVI-I/XGA adapter.
- 4) Connect the LAN input to the network (see scheme, cable 3).
- 5) Connect the ISDN inputs to the network terminations. (see cabling scheme, cable 4)



Connect the ISDN input (ISDN connector or network interface) only to a network termination (NT1).
Do not connect the equipment to an external telecommunications line.

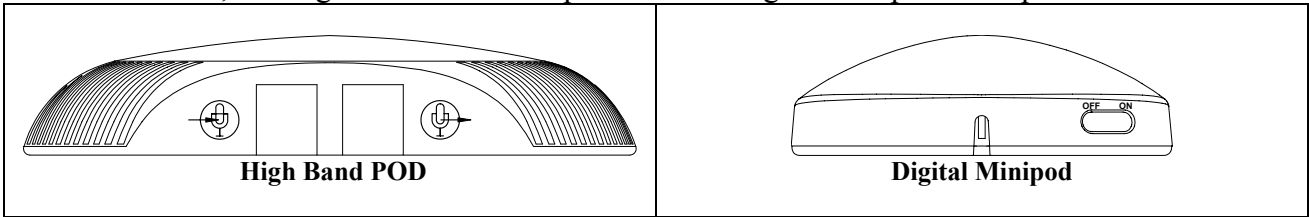
- 6) Connect supplementary audio or video equipments to the available inputs/outputs.
- 7) Connect the power supply (see cabling scheme, cable 5).
- 8) Switch the TV monitor ON.
- 9) Press the switch on key on the System rear.
- 10) Wait for the main user interface to appear.

The system status LED on the front means:

- **LED on:** System is on and normally operating.
- **LED flashing:** System power is on, but the System is in “standby” mode.
- **LED off:** System power is either off or not connected.

Connecting the Aethra POD

How to connect, the High Band Pod microphone or the Digital Minipod microphone.



If you use High Band Pod

Connect the High Band POD output  to the rear panel of the System.

If you use Digital Minipod

1. Connect the POD output (RJ12) to the rear panel of the System.
2. Switch the Digital Minipod ON.

Note

the point of connection and the power switch are in the rear Minipod.

Operation and use

This section of the manual explains the basic functionality of the System.
It is assumed that the system is correctly installed.

First time equipment is switched on

When the equipment is switched on for the first time, the following will appear on the screen:



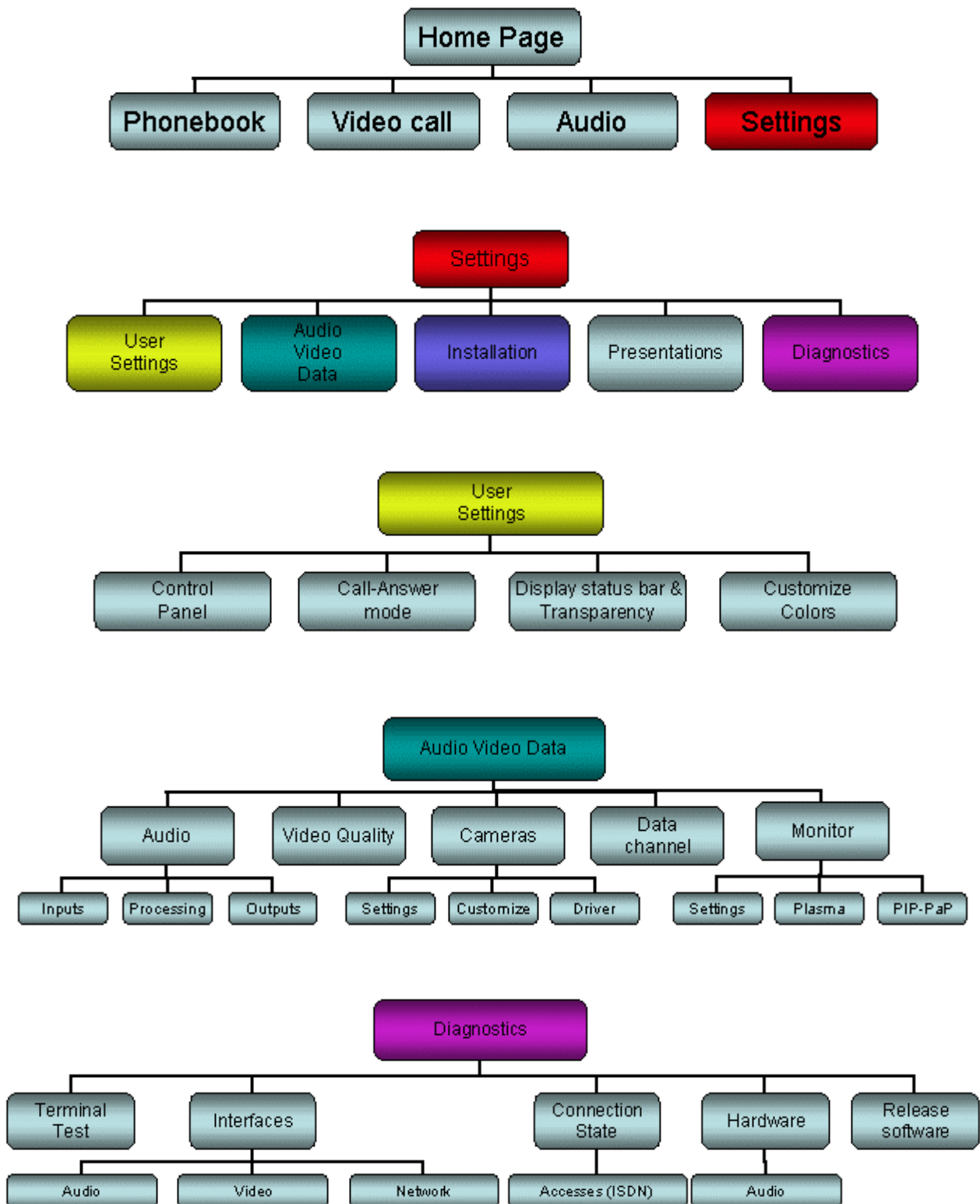
This allows the user to select :

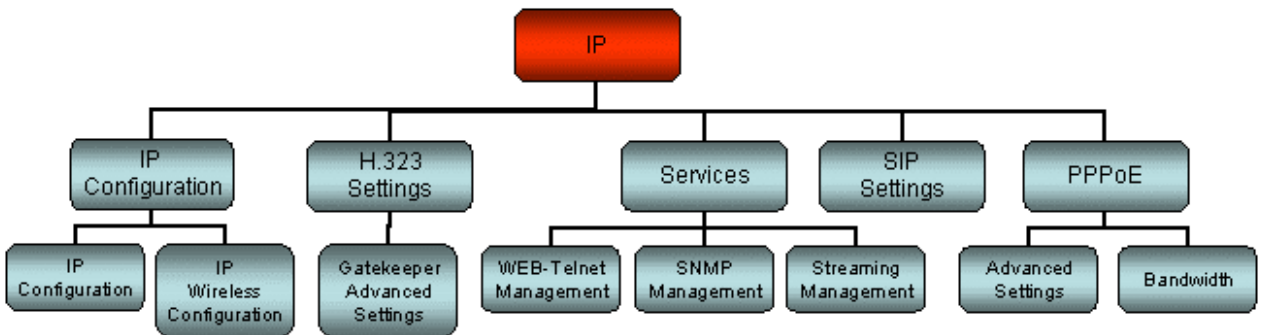
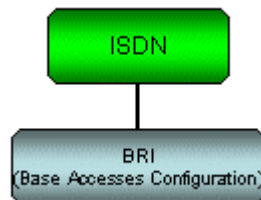
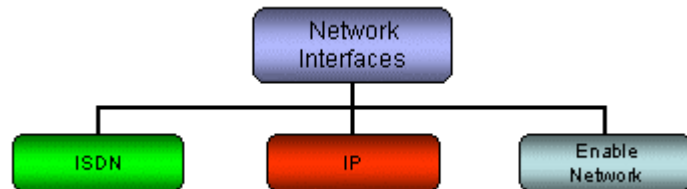
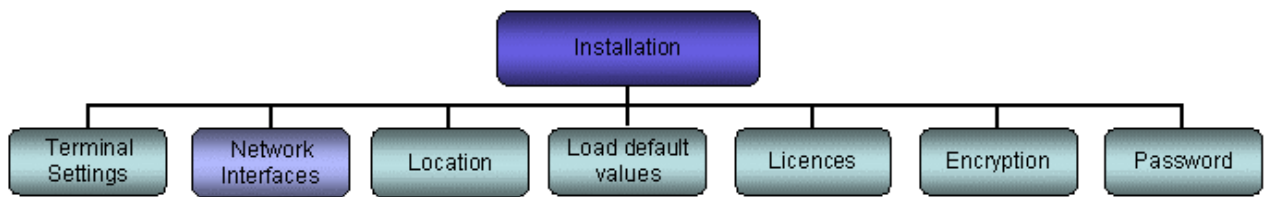
- Terminal Name
- Country
- Language
- PBX
- Audio Coding
- Video Standard
- Selection Tone
- Camera Frequency

- **Date and time settings**

By means of arrow keys select time on the control bar, and press OK: insert date and time.

Menu structure





How to make a call

Once the System is on, the main user interface will display the **Home Page**:



A call can be made in three different ways:

- From the Phonebook
- Audio/Video
- Audio Only



To make an IP call , the address of called IP terminal must be inserted following this syntax:
XXX.XXX.XXX.XXX

How to make a call from Phonebook

To enable the quick selection of a number to call, a phonebook is available to store data about terminals that are frequently called. To call one of these numbers, users need only select the entry in a list.

From the Home Page, using the arrow keys on the remote control device, move the pointer over the “Phonebook” icon and press OK.

The following image will appear:



Note:

The remote control has a dedicated key to directly open the phone book. See the “Remote Control” section.

To make a call:

- 1) Use “Search” field for an alpha-numeric search
- 2) Select the name, press OK to confirm
- 3) Move down to the chosen name and press OK to confirm.
- 4) Move to the CALL icon and press OK to make the call. The same function can be achieved by pressing the CALL remote control key.
- 5) In order to end the call, use the DISCONNECT remote control key. The system will ask you to confirm disconnection.

Audio-video calls

From the Home Page, select the VIDEO icon. The same function can be achieved by pressing the CALL key on the remote control.

You will enter the following page:



To complete the video call, follow these steps:

1. Select the call type from the dropdown menu (ISDN, IP-H323, IP-SIP).
2. ISDN only: check or uncheck the “56K” box for multiple rates of 56Kbps or 64Kbps.
3. Select the call rate from the drop-down menu .

! To select an option from a drop-down menu, it is necessary to go to the menu itself, press OK, select the desired option by means of the remote control arrows and press OK.

4. Enter the number or user alias (the H.323 Name from the “H.323 Settings” menu) you want to call using either the alphanumeric keys on the remote control or the virtual keypad.

!

1. A virtual keypad can be activated for situations where you need to enter text (e.g. names for the phonebook or aliases for calls).
2. To activate it, set the remote control cursor in the box where you want to enter text and press OK.
3. Select the desired letter by moving the cursor over it, and pressing OK.
4. To close the virtual keypad, select the ESC key and press OK

5. Move to the CALL icon and press OK to make the call. The same function can be achieved by pressing the “CALL “ key on the remote control.
6. To end the call, use the DISCONNECT remote control key; if configured, the system will ask you to confirm disconnection.

To Reselect an Incoming or Outgoing Call

Incoming calls are indicated with a red arrow while outgoing ones are indicated with a green arrow; a cyclic buffer of 60 numbers is available to store calls.

To reselect a called number press the CALL remote control key twice. A list will appear, and numbers can be selected and modified.

TCS-4 Mode Video Call

The TCS-4 mode is an H.320 call (ISDN) to a gateway which is able to transcode H.320 (ISDN)/H.323 (IP).

The format for number entry is:

“ISDN number of gateway” followed by “#” followed by “H.323 number (E.164) of the terminal to be called”.

Audio call

If you would like to make an audio-only call (using the System like a normal telephone), select the AUDIO icon from the Home Page.

To complete the audio call, follow these steps:

- 1) Select the type of call (ISDN, IP-H323, IP-SIP) from the drop-down menu.
- 2) Enter the number or the alias (IP) you want to call using the keys on the remote control or the virtual keypad.
- 3) Move to the CALL icon and press OK to make the call, or press the CALL remote control key.

To end communication, use the DISCONNECT remote control key: if enabled, the system will ask you to confirm disconnection.

Secure Connections


The System can manage secure videoconference sessions via encrypted connections, in both point-to-point and multipoint sessions. To do this, the encryption function must be enabled: for more information, refer to the “Encryption” section of this manual.


Once encryption is properly configured, you can make a secure call by following the same procedure described for a standard call.


Useful information:

The encryption status can be checked on the status bar.

If the encryption is enabled and configured, an icon showing a padlock is displayed on the status bar.

If the padlock is yellow and open () , encryption has been enabled but the function is not active.

If the padlock is green and closed, encryption is active ().

If the padlock is red and closed, encryption is activated only in transmission ().

How to receive a call

If you are in the Home Page and receive a call, a notification will be displayed in a window showing the caller's number. If the automatic answer function (described in a later section) is not enabled, you will be asked whether or not to accept the call. If you are in a different page, you will be asked to accept or reject the call whether or not the automatic answer function is enabled.

Dual Video Mode

Dual Video Connection

You can create a Dual Video connection to send two video streams originating from different sources.

!	This is feasible on the condition that the remote terminal supports Dual Video. Dual Video transmissions can be initiated by either the Audio-Video calling or called terminal. If the receiving terminal is set up with VGA/DVI-I output, and one of the received streams is an VGA stream, this one will be automatically displayed into VGA/DVI-I output. However, the user is able to switch the automatic disposition by pressing the “C” key on the remote control.
----------	--

To create a Dual Video connection:

- 1) Set up a normal audio-video connection with the desired terminal
- 2) Press the “Dual” key on the remote control
- 3) Select the desired second video input source from the drop-down menu
- 4) Move to the YES icon and press OK



Once Dual Video is activated, if the receiving terminal is set up with two monitors, the user will be able to see the two video streams simultaneously. If there is only one monitor, the user can switch between the video streams by pressing the “SELF” key on the remote control.

Dual Video Disconnection

To disconnect Dual Video only:

- 1) Press the “Dual” key on the remote control.
- 2) Move to the icon “Yes” and press OK.



Note

To disconnect the whole Videoconference press the “Disconnect” key on the remote control.

Using the Phonebook

System allows use of either a **local** phonebook or a phone book on a **remote server (LDAP H.350 protocol)**.

Entering Names in the Phonebook

From the Home Page, go to the “PHONEBOOK” icon and press OK, or press the “PHONEBOOK” remote control key.

Move the arrow keys to the ENTER icon and press OK.

The following page will be displayed:



Enter data in the phonebook by using the remote control alphanumeric keys or the virtual keypad to fill out the available fields.

- Choose the call configuration to record the connection details for this user (Interface used - ISDN, IP, SIP - and transfer rate)
- Enter NAME and COMPANY
- Enter the prefix and number
- Using the arrows move to the SAVE icon to save the new data or to CANCEL to exit and press OK

Note:

If you want to store an audio call only entry, you must check the Speech box.

Modifying and Erasing Phonebook Entries

To modify a phonebook entry:

- 1) Select the desired entry and press OK
- 2) Move to the MODIFY icon and press OK again
- 3) Enter modifications and save them

To erase an entry in the phonebook:

- 1) Select the desired entry and press OK.
- 2) Move to the CANCEL icon and press OK (the system will ask you to confirm deletion).

Connecting to a global Remote Phonebook

Phone book on a remote server (LDAP H.350 protocol).

To connect to the remote server, move to the drop down menu and select the desired server IP address. The phonebook will now operate as described above.

Note

To correctly configure remote server connection parameters, please contact your network administrator.

Video Input Management

It is possible to manage different video inputs by selecting them using the remote control keys “Camera”. The function keys “Red”-“Yellow”-“Camera”, can be configured to be associated with any available video input.

Possible choices include:

- Room camera
- VGA/DVI-I Video input
- Whatever video peripheral with composite signal (e.g. camera or VCR)

Note:

The desired video source must be connected to the System inputs on the back of the equipment beforehand. For a correct setup of the function keys, see the chapter “Audio-Video-Data”, section “Camera”.

During a connection it is also possible to control not only the local video camera’s zoom and panning functions but also those of the remote camera (if enabled). Use the remote control key “Far/Near” to select remote or local camera.

Field of View and Zoom

From the Home Page, using the remote control, go to the “video window” and press OK. Adjust the video camera’s field of view with the arrow keys and press OK on the remote control.

An alternate method:

From the Home Page, go to the “Magnifier” icon on the status bar and press OK. You will see a full screen display with the camera under your control.

To release camera control, press OK.

Using the VGA/DVI-I IN/OUT

In the system rear panel there are one **VGA/DVI-I** input to connect a personal computer, and one **VGA/DVI-I** output for connect a monitor. For a correct cabling, see the “cabling scheme”.

Correct use of the **VGA/DVI-I** implies that the video PC configuration has been set (setting: screen→ properties) with one of the following picture frequency limits (or refresh frequencies).

Resolution	Refresh Frequency (Hz)
640 x 480	60, 70, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1024 x 768	60, 70, 72, 75, 85
1280 x 1024	60, 70, 75

Video Privacy

Once in connection.

To activate the Video Privacy function, press the “VIDEO PRIVACY” key on the remote control. Local video will no longer be transmitted.



The icon will appear in the video window indicating that the remote terminal is no longer receiving video from local terminal.

Not in connection


Activates/Deactivates:

Video privacy as above.

Do Not disturb System does not answer to incoming calls (busy for the remote)

Controlling audio

The “VOLUME (+ and -)” keys allow you to adjust the level of received audio.

By pressing MUTE key you can activate the mute function, that is local audio will no longer be transmitted. On both the local and remote displays, the icon  will appear, indicating that the mute function is active.

Video camera presets

The Preset function allows the user to save camera positions (up to a maximum of 122 positions) in order to enable quick selection of a certain camera frame.

To save a preset:

- 1) Set the desired camera position and adjust the video zoom.
- 2) Press the “MEMO” key on the remote control and choose a memory location (maximum two characters)

To recall a memory location:

1. Press the “SEL” remote control key
2. Using the remote control key, enter the memory location number corresponding to the desired preset.

Note:

The preset includes both the selected camera and its position, so recalling a preset can change the current video camera.

Besides, from remote, the protocol of control of the camera allows to recall only the first 16 memorized preset.

System Configuration - Settings

This section describes the procedures to properly configure the System.

Note

that some configuration parameters can be modified only when no connection is active.

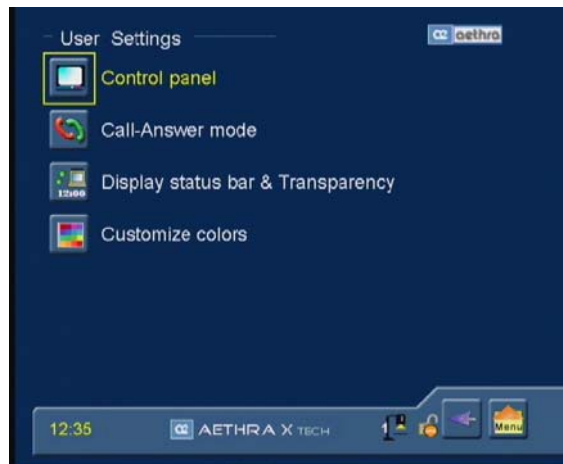
From the “Home Page”, with the remote control, select the icon “Settings” and press “OK”.

User preferences

From the “Home page” select:

1. SETTINGS
2. USER SETTINGS

The following page will be displayed:



From here you can access the following submenus:

- Control Panel.
- Call-Answer mode.
- Display Status Bar & Transparency.
- Customize colors.

Control panel

In these pages you can configure some system parameters.

Display

- **Local Information:**
If activated, shows information such as terminal name, ISDN number, and IP address on the monitor in graphical form
- **Show Warning:**
If activated, allows visualization of “Bonding Recovery” messages
- **Show logo when in a call:**
Enables/disables logo display during a call. Logo is customizable—default is Aethra S.p.A.
- **Disable still picture:**
disable transmission/receiving of “still images”.

Screensaver

- **Automatic screensaver:**
to enable/disable the automatic screensaver function, and to set its timeout

Remote control

- **Numeric only remote control:**

Enable\Disable **alphabetical digits only** on the remote control

- **ID code:**

In order to control more systems with only one remote control, you can assign to each system a numeric code (01 to 99), and then consequently set the remote control.

- To configure the system:
 - a. the system code appears in the page
 - b. Is possible modify or save the new code.
- To configure the remote control:
 1. Press the “RED” and “GREEN” keys at the same time
 2. Wait for “Stand by” key stopping blinking
 3. Insert the numeric code (01 to 99)

Call-Answer-Mode

General

This menu contains the following configuration settings:

- **Mute**

selected, at the start-up and after each disconnection system will not transmit audio, an icon will be displayed in the local and remote terminals.

- **Do Not Disturb**


selected, at the start-up and after each disconnection system will not accept incoming calls, an icon will be displayed in the local terminal.

- **Video Privacy**

- **Once in connection.**

To activate the Video Privacy function, press the “VIDEO PRIVACY” key on the remote control. Local video will no longer be transmitted.



The icon  will appear in the video window indicating that the remote terminal is no longer receiving video from local terminal.

- **Not in connection.**

Activates/Deactivates:

- **Video privacy** as above.

- **Do Not disturb** System does not answer to incoming calls (busy for the remote)

- **Confirm disconnection**

Enable/disable confirmation requests for call disconnection.

- **Enable Tones**

Enable/disable tones in phase of call.

- **Automatic answer:**

Enable/disable the automatic answer function, after the selected number of rings.

H.320

This menu contains the following configuration settings:

- **Audio Number = Video Number:**
In a non-aggregated ISDN call, the audio number may be different from the video number. If this checkbox is not selected, the System will request the video number and offer by default the same number as the one used by audio.
- **Additional Calls:**
Select automatic or manual configuration of additional calls
- **Mode:**
Allows you to set the call mode to 64K or 56K.
- **TCS4 Delimiter**
definition of TCS4 calls delimiter: “#” or “*”. TCS4 is a special routing method for direct video call when a Gateway is present on the network (ISDN network to IP network). To place a call using a TCS4 extension, do the following:
 1. Obtain the following information: Gateway number, delimiter and TCS4 extension.
 2. Dial the Gateway number, the delimiter and the TCS4 extension.
Example: ISDN_Gateway_number# TCS4_extension.

Broadcast

This menu contains the following configuration settings:

- This option allows you to set a transmission as “broadcast” (without capabilities exchange).

Note:

In order to make a Broadcast call, the two terminals must have the same audio, video, rate and Data (LSD) configurations.

Display Status Bar and Transparency

- **STATUS BAR:**
Allows you to personalise the System graphical interface, choosing whether you want the status bar to be present and, if so, what information should be displayed on it.
Information on the status bar:
Date and Time, selected camera, channel status, charges, data channel.
- **TRANSPARENCY:**
allows you to add transparency to graphical pages where the video window is not reduced in size.
This transparency can be set to four different preset levels (high=75% transparency, medium=50%, low=25%, opaque=0%). Transparency can be used in different ways:
 - 1) Automatic: (default) Only the diagnostic pages of the “Connection state” uses transparency with a selectable initial level (default medium). The transparency level can be changed dynamically.
 - 2) Variable: All pages where no video is present use a selectable initial transparency level (default medium). The transparency level can be changed dynamically.
 - 3) Fixed: All pages where no video is present use a selectable initial transparency level (default medium). The transparency level cannot be changed dynamically.
 - 4) Off: Transparency is always deactivated.

Dynamic change of transparency level is achieved by pressing the remote control key C. The transparency is always deactivated when a page is superimposed with a message page to improve legibility.

Customize colors

- Allows personalization of the **graphical interface colours** of the System.

Audio – Video – Data

From the Home Page select:

1. SETTINGS
2. AUDIO VIDEO DATA

The following page will be displayed:



You can access the following submenus:

- Audio
- Video Quality
- Cameras
- Monitor
- Data channel

Audio

You can access the following submenus:

- Inputs
- Processing
- Outputs

and adjust the ringing and sound volume.

Volume for Ringing and Sound.

For adjust the **ringing** and **sound volume**, follow these steps:

1. Select AUDIO or RINGING from the “Volume” dropdown menu.
2. Use the remote control arrow keys to move the Volume slider control.
3. Choose the desired value, using the remote control arrow keys.

Inputs

Allows for the adjustment of each audio input to the System.

Move to the desired input and press OK, a window will appear where you can:

- Set the gain value for the input
- Enable/disable the input audio stream
- Enable/disable the Echo Canceller

The icon “**load default values**” restore factory values of the audio inputs enabling all the audio inputs.

Processing

In this menu you can enable/disable the Echo Canceller functions:

- AGC.
- Noise Reduction.

Outputs

In this page you can configure audio flows sent to the System Audio outputs.

You can first select Audio outputs from drop down menu, and then select the audio flow you want to send to the desired output.

To restore factory values click on “Load default values” icon.

Video Quality

From the Home Page select:

1. SETTINGS
2. AUDIO VIDEO DATA
3. VIDEO QUALITY.

This allows the configuration of the following parameters:

- **“Video Quality-Speed”:**
To balance between sharpness and dynamic nature of video images.

- **“Aethra Error Strategy”:**
Set the number of allowed line errors before video is frozen:
 “Min Fluency”: stop video at the first occurred error,
 “Max Fluency”: never stop video and allow errors through.

- **“Audio Delay Automatic”:**
You can also **synchronise audio with video**. The audio delay represents the value in milliseconds by which received audio is delayed.
In order to have perfect synchronisation between audio and video, it is necessary to adjust these parameters according to the connection type.
By selecting the check box (strongly recommended option), you allow this operation to be performed automatically by the system. Alternatively, you can make manual adjustments by moving the slider along the bar until you obtain the best synchronisation.

Cameras

This menu allows you to:

Settings

- Enable/disable the **“remote control”** of the local camera.
- Select, from dropdown menu, the video input.
- Set the values for contrast, brightness and colour in order to obtain a better video image.

A preview window allows the immediate control of changes.

Customize

Each **input** could be enabled\disabled (that is, inserted in a selection list), associated to a Name, associated to a shortcut (RED, YELLOW, Camera keys on remote control) for a quick choice.

To choose a shortcut, select the related icon and press OK.

For the **VGA/DVI-I input** from the dropdown menu you can chose:

- Analogic (**analogical DVI** signal input enable)
- Digital (**digital DVI** signal input enable)
- Automatic (default; **analogical and digital DVI** signal input enable)

(For VGA/DVI-I input, see cabling scheme)

Driver

Advanced (Administrator Password Required)

Select driver for Room Camera and other Video Input, and enable the PTZ function(check “MOVE”) for all video inputs.

Monitors

In this page is possible to configure system video outputs.

You can access three menus:

- Settings
- PiP-PaP
- Plasma

Settings

In this page you can set following system parameters:

- Monitors Number
- Monitor Menu
- Video outputs

Dropdown Menu “**Monitors Number**” (default setting: Automatic).

Following table shows all available configurations:

Dropdown menu ” Monitors Number”	Connected monitors
Automatic	System automatically recognises connected monitors
TV1	One analogical monitor
HighDefTV	One VGA/DVI-I monitor
TV1+ HighDefTV	One analogical monitor and one VGA/DVI-I monitor

Dropdown Menu “**Monitor Menu**” (default setting: Automatic).

In case the “TV1+ HighDefTV” configuration has been choosen, so to have two monitors connected to the system, is possible to choose where to see GUI (Graphical user interface).

Available configurations are:

Automatic	GUI set by the system
TV1	GUI always on TV1
VGA	GUI always on VGA

Video outputs

TV1: connect a monitor or an analogical TV to TV1 video output (RCA connector, point 2 of connections diagram). If you select **16:9 check box**, the system adds vertical side banners in order to scale fullscreen video image from 4:3 to 16:9.

VGA/DVI-I: connect a monitor with a VGA/DVI-I connector to VGA/DVI-I video output. Choose in dropdown menu used monitor (VGA out in connections diagram). **16:9 check box** (use only with 16:9 monitors). If you select **16:9 check box**, the system adds vertical side banners in order to scale fullscreen video image from 4:3 to 16:9.

Available VGA/DVI-I output resolutions are:

VGA resolutions
1280x768
1024x768
800x600
640x480

HDTV resolutions
720p
576p
480p

In case of digital DVI monitor usage, user **must check box “DigitalDVI”**.

PiP-PaP

In this page is possible to select **“Multi Imagine”** system functionalities:

- **PiP: Picture In Picture**

Allows to see two overlapped images in one monitor, that is remote image in full-screen format, an local image in a smaller overlapped window; by means of remote control “Self” key you can switch windows content.

Is possible to choose:

- PiP position (one of four monitor corners)
- PiP movements (clockwise or counterclockwise) by means of remote control “PiP” key
- **PaP: Picture and Picture**
Allows to see in one monitor two windows side by side, with local and remote images; by means of remote control “Self” key you can switch windows content.
- **Multi Imagine Type**
 - a. By selecting **AUTO** a mixed PiP and PaP function is enabled.
By means of remote control “PiP” key you can switch between PiP and PaP.
 - b. By selecting **PiP** PiP function is enabled.
 - c. By selecting **PaP** PaP function is enabled.



Multi image type must be enabled separately for TV1 and HighDefTV monitor

- **Multi Imagine Mode**

- a. By selecting **AUTO** PiP and PaP functions are enabled only when needed, that is when number of video flows is greater than available monitors number, and automatically place video flows (with precedence to remote ones).
- b. By selecting **ON** PiP and PaP functions are enabled if at least two video flows are available (in case of unique video flow you have a full screen image, eg when system is not connected)
- c. By selecting **OFF** PiP and PaP functions are disabled.



Multi image mode must be enabled separately for TV1 and HighDefTV monitor

- **Multi Imagine: remote control “Self” key and monitor info.**
Remote control “Self” key allows to show video flows in different available monitors, choosing among different combinations.
In the lower right corner of monitor containing GUI, an icon appears with four white monitors showing available configurations, active configuration being in red.
The icon is hidden when default configuration is active.

Plasma

Select plasma, type of monitor and viewing modality.

Note.

The follows instructions refers “Pioneer” monitors.

! Please carefully check VGA/DVI-I, Y/C and RS232C/DEBUG (null modem cable) connections between plasma and System.



- In the “Type” field, set the plasma model
- In the “Number of monitors” field, select the number of connected plasma monitors
- In the “Mode” field, select the default viewing mode from the pop-up menu.

! First time “Plasma type” is selected (usually factory done), a particular operations sequence must be followed:

1. Do not connect the system and the monitor by means of serial cable.
2. Select plasma type.
3. Once completed all initializations, switch off the system, connect the system and the monitor by means of serial cable, switch on the system: now is ready.

Viewing modes

Different viewing modes may change depending on used monitor characteristics .
Following viewing modes with corresponding short explanations refer to Pioneer systems.

1. **Automatic MultiScreen**
2. **Fixed MultiScreen**
3. **Automatic BigLittleScreen**

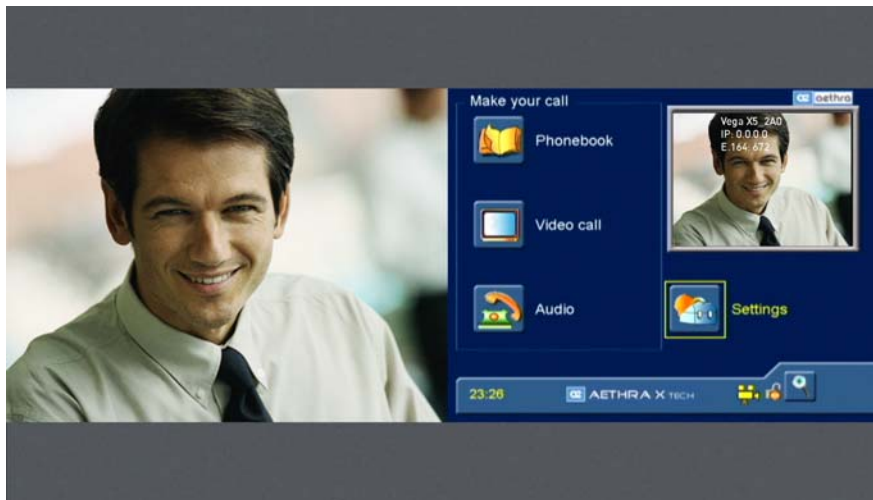
1) Automatic MultiScreen

Selecting this mode, the system shows two side-by-side equal-sized pictures: graphics relating to system management will appear on the right, whereas motion video will appear on the left. Once connected, an XGA remote signal automatically changes the viewing mode to BigLittleScreen mode; once in this mode, surfing inside menus will let back again to the MultiScreen viewing mode.

To see a local XGA image select full-screen visualization, then you can switch to BigLittleScreen mode by pressing the “C” key on the remote control.

Exiting from the FullScreen mode, the system immediately comes back to the MultiScreen viewing mode.

a) Disconnected system.



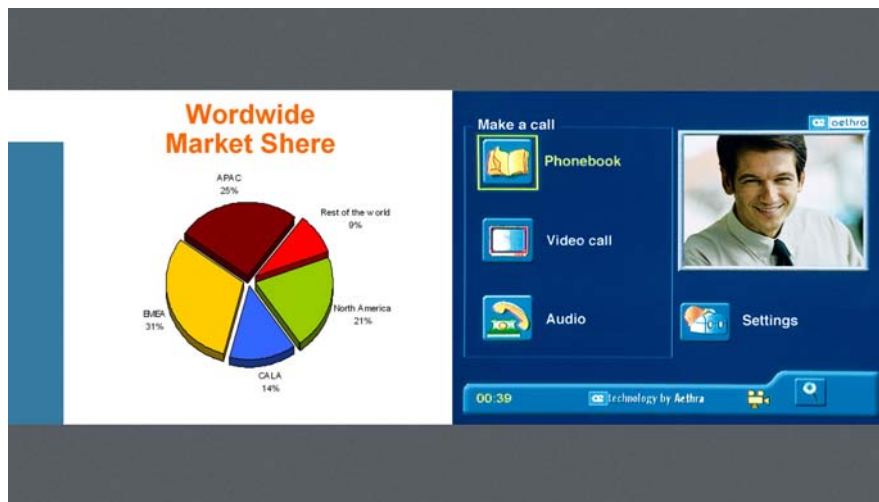
b) Connected system (with 50" Pioneer plasma, you'll obtain two 27" images, 4:3).



c) Connected system that receives a remote XGA image (with 50" Pioneer plasma, you'll obtain two 4:3 images, a big one (42") with 1024 x 768 XGA resolution image and a small one (11").



d) Connected system with remote XGA image, while local user looks at the menu.



e) Connected system with remote XGA image, in DualVideo XGA mode. The larger pane displays the XGA image, while the smaller one displays the remote wide stream.



2) Fixed MultiScreen

Selecting this mode causes the system to display two side-by-side, equally-sized frames. Graphics relating to system management will appear on the right, while remote video (or XGA) appears on the left.



3) Automatic BigLittleScreen

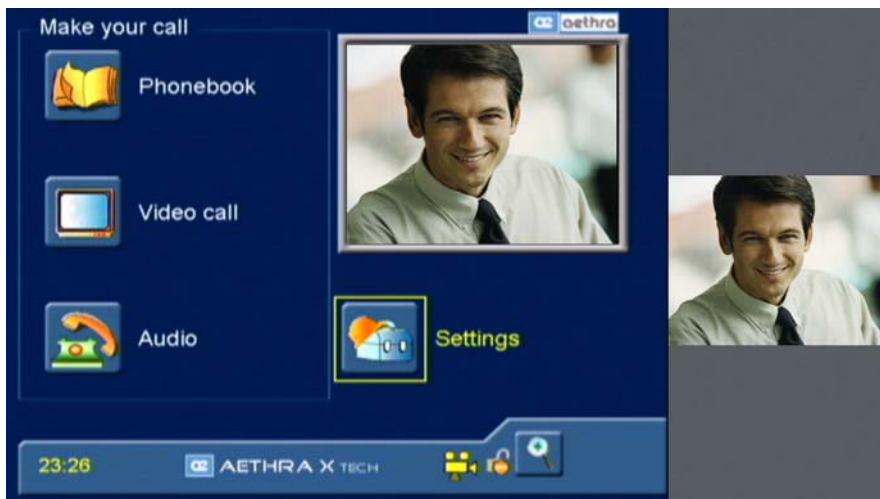
If this mode is selected, the system will show two video outputs in different-sized frames.

The larger frame on the left will show the graphics relating to system management, while the video stream will appear in the smaller frame on the right.

During an active connection, the system automatically selects which video stream to place in the larger frame.

The initial viewing mode can be restored only via the menu.

a) Disconnected system.



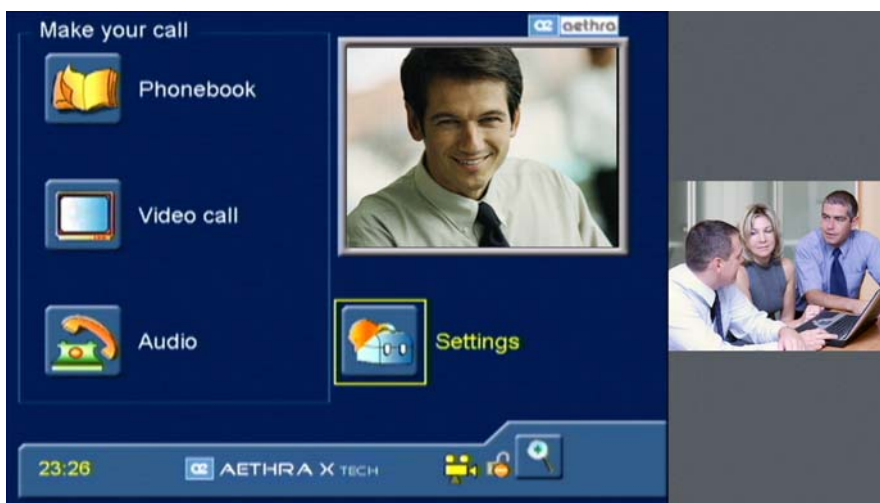
b) Connected system.



c) Connected system that receives an XGA image.



d) Connected system while user browses the menu.



e) Connected system that receive an XGA image on Dual Video XGA mode.



Data Channels

From the “Home Page” select:

1. SETTINGS
2. AUDIO – VIDEO – DATA
3. DATA CHANNELS

In this menu you can:

- Enable or disable “Data” transmission.
- Select the transfer rate.
- Enable or disable “Modem function” (if activated allows AT commands usage).
- Choose the “data channel max rate” (only H.320).

High	Max data, no audio, no video. Data channel optimisation to the detriment of both audio and video
Medium	Max data, audio, no video. Data channel optimisation to the detriment of audio (video still active)
Norm	Max data, audio, video. Data channel optimisation, with both audio and video active.
Auto	Data, audio, video. Data channel rate optimisation to RS232 rate and connection speed.
Select Rate	User can choose the data channel rate.

- Choose “MLP” data transfer protocol

Installation

From the “Home Page” select:

1. SETTINGS.
2. INSTALLATION.

You will be prompted for a password.

The password is required to avoid accidental modifications and changes to settings.

Password

There are three different kinds of passwords:

Administrator password: Always active. Can be modified by pressing the “EDIT” icon.

User password: Must be activated. Can be modified by pressing the “EDIT” icon.

Phonebook password: Must be activated. Can be modified by pressing the “EDIT” icon.

Note:

TheDefault password value is “1234”.

Encryption

From the “Home Page” select:

1. SETTINGS
2. INSTALLATION
3. ENCRYPTION

The configuration menu will be displayed; here you can set the following parameters:

Use Encryption:

If encryption is activated, the System will use encryption in either H.323 or H.320. It is also possible to enable/disable the encryption from the toolbar: select the padlock icon, and press OK.

For IP calls

- If encryption has been activated, the data protection procedure is active from the beginning of a videoconference.

Encryption is active from start (ISDN):

- If this option is selected, the System executes the encryption procedure from the beginning of the ISDN connection.
- If this option is not selected, the ISDN connection starts in unencrypted mode. Encryption can be activated later at any time during the connection. To do this, select the yellow padlock on the status bar and press OK.

Unprotected calls

From this drop-down menu you can choose the policy the System will apply if the remote terminal is not able to support protected calls.

- **Disconnect** – The System will not allow connection with a remote terminal that does not support encryption, and therefore automatically disconnects.
- **Ask Confirmation** – During the session negotiation phase, the System will ask you to confirm that you want to establish an unprotected call.
- **Inform** – The System will inform you that you are about to establish an unprotected connection by displaying a visual warning message.
- **State** – The System will notify you that you are about to establish an unprotected call, and once the connection is established an open padlock symbol will be displayed on the status bar.

Length of AES Key (ISDN only)

From this drop-down menu you can choose (for ISDN connections only) three AES key lengths:

- 128 bits
- 192 bits
- 256 bits
- <Auto> (allows optimal choice according to the characteristics of the terminals negotiating the videoconference session.)

Note

For an IP connection, the key length is always 128 bits.

Length of Prime DH Number Key (ISDN Only)

The encryption protocol requires the simultaneous exchange of a prime number and an AES private key between terminals.

For H.320 calls you can choose between two prime number lengths:

- High Security (length 1024 bits)
- Very High Security (length 1536 bits)

Note

For IP calls, the System always uses the High Security option with a 1024-bit length.

Most common video communication terminals normally use the High Security prime number length and the 128-bit AES private key.

Licenses

From the Home Page select:

1. SETTINGS
2. INSTALLATION
3. LICENSES

This page is dedicated to supplementary functions not offered by default. In order to obtain information on the activation of these functions, please contact your system supplier.

To insert a licence key by means of the remote control:

1. Enter the licence key.
2. Press the “Enable Licence” icon.

Terminal Settings

From the Home Page select:

1. SETTINGS
2. INSTALLATION
3. TERMINAL SETTINGS

In this section you can configure terminal settings for various network interfaces. For each interface it is possible to set, if present:

- The maximum data **“Rate”** for a call (excluding NIC).
- **Audio coding**
Enable/disable G.722.1 and MP4 AAC-LD coding.
- **Video coding**
Enable/disable H.264 coding
- **Channels**
Determine if channels are to be bonded or not (ISDN only).

Note

With audio and video encoder/decoder settings set to <Auto> the system choose the encoder/decoder based on the connection bit rate.

DualVideo H.239 and **DuoVideo™** can also be enabled/disabled.

Network interface

From the Home Page select:

1. SETTINGS
2. INSTALLATION
3. NETWORK INTERFACE

In this section you can choose and configure the system’s network interfaces. For each interface, it is possible to set some parameters.

ISDN network interface

In this section you can:

- Select the “**Euro**” or “**National**” protocols
- Select Access type:
 - **BRI** Access
- Activate/deactivate:
 - **CLIR** (Calling Line Identity Restriction): if enabled, system will not transmit its number when establishing a call.
 - **COLR** (Connected Line Identity Restriction): if enabled, system will not transmit its number while receiving a call.
- Activate or deactivate the “**Downspeed**” function that is automatically called when one or more lines are dropped during a call.
- Activate the “**FALLBACK**” function in order to allow a phone call when the remote system is a basic telephone.
- Enable/disable the “**Bonding Recovery**” function in order to cope with a situation in which network errors (such as network SLIP errors) occur during a bonding connection.

In a call, following messages could appear:

- Corrupted video received. Please wait...
- Video received Ok.
- Corrupted data received. Please wait...
- Data received Ok.
- Network error recovery: re-establishing call...
- Call established. Please wait...
- Down-speed, connection rate
- Activate or deactivate the **5ESS** protocol (for National ISDN only).
- Select the mode (64K or 56K).
- Activate or deactivate the **1TR6** function (allows you to change the protocol level 3 from **ETS1** to **1TR6**, for Euro ISDN only).
- Activate or deactivate the **QSIG** protocol (ISDN signalling protocol).
- Configuring accesses.

Access Configuration (ISDN BRI Euro)

Move to the Configure Access icon and press OK.

From this menu, you can:

- Choose to **enable access**.
- Specify the **number to be associated** with the access.
- Specify the **subaddress**, if present.
- Choose to enable the “**MULTINUMBER**” function by checking the appropriate box.
- Select **TEI** (either Automatic or Fixed)

The TEI is an identifying number that allows the ISDN exchange to distinguish between different terminals connected to a common access point. If TEI Fixed is selected, then you must manually enter the TEI number. Conversely, by not selecting it, the parameter will be set as TEI Automatic. In this case, the TEI number will be automatically assigned by the exchange and no further operations in this menu are necessary.

Note

Normally, the TEI is left as AUTO because an incorrect setting could create connection problems

Access configuration (ISDN BRI National)

Move to the Configure “Access” icon and press OK.

From this menu you can:

- Choose to **enable the access**.
- Specify the **number to be associated** with the access.
- Specify the **SPID**, if present.
- Select **TEI**, either Automatic or Fixed.
- Enable any eventual **SPID2** and enter the appropriate numbers.

IP configuration

From the Home Page select:

1. SETTINGS
2. INSTALLATION
3. NETWORK INTERFACES
4. IP

The following page will be displayed:



The five available options are:

- IP Configuration.
- H.323 settings
- SIP settings
- Services
- PPPoE

IP Configuration

This menu is for Integrated LAN and Wireless LAN configurations; select “IP Configuration” and select the type of the desired LAN Network:

- Select “IP Configuration” (Integrated LAN)
- Select “IP Wireless Configuration” (Wireless LAN _ for “X3 Wireless version” only)
- Select the Priority between fixed and wireless network, for outgoing calls.

IP Configuration: Integrated LAN

In this menu, you can enable/disable automatic assignment of an IP address:

- IP address;
- Subnet mask;
- Gateway IP address;
- DNS server IP address.

Is possible to configure Ethernet port either for what concerns connection “LAN speed” (10Mbps / 100Mbps), or “Duplex Mode” (Half / Full), in order to optimally operate with HUB/Switch that do not support automatic configuration.

Default configuration is <Auto> for both settings.

!	For configuration information, please contact your network administrator.
----------	--

By selecting ADVANCED, you can enter a page to set:

- The range of **dynamic TCP and UDP ports (*)**.
- The **quality of service** policy to be applied:
 - **IP Precedence/TOS**
 - **Differentiated service**. You can choose audio and video values in a 0 to 63 range
- “Use NAT”:
 1. “NAT Type” should be set to “Others”
 2. “Public IP address” must be the public IP address of the NAT.

By selecting the “BANDWIDTH” icon is possible to enable and set maximum bandwidth usage limits (in Kbps). These limits can be different in transmission and reception, a very useful function on ADSL networks.

Firewalls

All Aethra videoconference systems have been tested with:

- Cisco PIX Firewall (Firewall H.323 compatible - release 6.1 or later).
- Cisco MCM Proxy (NAT H.323 compatible - IOS release 12.2 or later).

Note (*)

when a firewall is crossed, the firewall administrator must open a range of dynamic TCP and UDP ports, as configured in the system, to allow bidirectional IP traffic. Moreover, once the ports have been opened, the protocols (TCP 1720 (Q.931), TCP 1503 (T.120), UDP 1719, and 1718 (RAS)) involved in a call must be taken into account.

IP configuration “Wireless” (for “X3 Wireless version” only)

In this menu, you can enable automatic IP configuration, or enter the following data manually:

- IP address;
- Subnet mask;
- Gateway IP address;
- DNS server IP address corresponding to a wireless network.

!	For configuration information, please contact your network administrator.
----------	--

By selecting **ADVANCED**, you can enter a page to set:

- **SSID:** wireless network identification.
- **MODE:**
 - Ad-Hoc:** all terminals in the network communicate with each other, and not with a dedicated access point.
 - Managed:** all terminals present in the network communicate with an access point.
- **ENCRPTION MODE:** enable/disable encryption and allow user to set the desired key length.
- **ACTIVE KEY:** select one of four alternative keys.

By selecting the “**BANDWIDTH**” icon it is possible to enable and set maximum bandwidth usage limits (in Kbps). These limits can be different for transmission and reception, a very useful feature on ADSL networks.

H323 Settings

This section contains the configuration options necessary to use the system with the H.323 protocol:

- **Name H.323:** (H.323 ID) the name used by the terminal for registration with the gatekeeper.
- **Number H.323:** (E.164) identifying number used by the terminal for registration with the gatekeeper
- **Gatekeeper** use and address
 - Gatekeeper automatic IP address
 - Gatekeeper static IP address
 - Advanced:** Automatic registration to Gatekeeper: allows the user to change registration timings
- **Using NetMeeting:** If a T.120 connection is available, a data conference using NetMeeting can be started by entering the IP address of the application host server. To enable this function:
 1. Check the box next to “Use NetMeeting”
 2. Enter a server IP address where the application is hosted.

!	For configuration information, please contact your network administrator.
----------	--

SIP Settings

This section contains the configuration options for use of the system with the SIP protocol:

- Terminal **name**
- Terminal **Password**
- **SIP Registrar Server**
 - “Use registrar”: run terminal registration at a SIP Registrar Server
 - “Name”: Enter SIP Registrar Server name
(Ex: SipRegistrarServer.Domain.xxx)
 - “IP Address”
 - “Duration”: Registration duration (in seconds).
 - “Port”: Port for server signalling. (Default is 5060).

- **Sip Proxy Server**
 - “Use Proxy”: use a Sip Proxy Server
 - “Name”: Enter Sip Proxy Server name (ex: SipProxyServer.Domain.xxx)
 - “Domain”: Enter Sip Proxy Server domain
 - “IP Address”
 - “Port”: Port for server signalling (Default is 5060).



For configuration information, please contact your network administrator.

Services

The System allows for the configuration of various parameters associated with web management, SNMP management and streaming management.

Web-Telnet management

In this section you can:

Enable/disable System access from the Web using Telnet by means of IP, ISDN connections

- Enable/disable phonebook management from the Web.
- Enable/disable phonebook management from the Web via ISDN(default: enabled)
- Limit access to a single IP address or any IP address in a specified network.
- Change the Web/Telnet access password (default: Username Aethra, Password 1234).

SNMP Management

In this section you can:

Enable/disable SNMP use.

- Enter Administrator name.
- Enter Location.
- Limit editing of settings to one IP address, or any IP address on a specified network.
- Limit reading of settings to one IP address, or any IP address on a specified network.



For configuration information, please contact your network administrator.

Streaming Management

In this menu the System can be configured to use streaming. This technology allows viewing of and listening to live or recorded events by a large number of users connected to the IP network without the need for a large file to be downloaded. It is based on the continuous transmission of data compressed by particular programs (systems) from a server, then decoded at the client side by an appropriate player that works even during data buffering, thereby avoiding long delays.

The System is able to transmit to networks in either unicast or multicast. If the streaming is unicast, only one client at a time is allowed to connect to the stream. If it is multicast, there is no theoretical limit to the number of connected clients.

In case of pre-recorded event streaming, replay a recording of the event using a VCR or DVD player connected to the System video input available for this purpose, select this input and begin the streaming.

Note that the system does not act as a distribution server, rather as a simple system. It does not provide connections using RTSP (Real Time Streaming Protocol), nor can it provide unicast streaming to multiple clients, or offer other services typical of distribution servers.

Streaming is supported by RTP (Real-time Transport Protocol). Video packets are encoded in H.261, while audio packets are encoded in G.711.

Menu options are "Streaming Management," "Enable Streaming," and Activation.

“Streaming Management”

Allows modifications of the Announcements, Video, Rate, Address, Port, and TTL/Hops parameters by external applications (from the Web, for example). If this option is not selected and a unicast IP address is present in the “Address”, then only the system identified by that IP address will be able to view the stream.

- **Enable all addresses:** this option allows modifications to the previously mentioned parameters by almost any external system. If this option is not selected, then you can establish which system or subnet is enabled to perform this operation. If the mask is 255.255.255.255, then the system will be selected, if the mask is 255.255.255.0 then the subnet will be selected.
- **Password:** allows password protection of streaming management

“Enable Streaming”

Allows stream viewing according to the limitations imposed by the parameters “Streaming Management” and “Enable all addresses.” If this option is not selected, streaming will never be activated.

Announcements

This drop-down menu allows you to choose how the System will notify the user that an external system has requested streaming activation.

Options:

- **Activation:** The System will display a dialogue box containing a warning and a video camera icon that will stay in place as a reminder for as long as streaming is active.
- **Status:** Only the video camera icon will be displayed during streaming.
- **Confirmation request:** A dialogue box will appear to request confirmation of streaming activation. This option offers an extra level of protection.

Video

This drop-down menu allows you to choose which video signal is transmitted when streaming is active.

If the “**Automatic**” option is selected, the streaming content will be determined by the status of the terminal: if the terminal is connected (in either a point-to-point or multipoint session), video coming from the remote site will be streamed. If the terminal is disconnected, local video will be streamed. If the “**Local**” option is selected, the system will always stream local video.

Rate

This drop-down menu allows you to choose the bandwidth occupied by audio and video streaming. Note that if a rate of 64K has been selected, the video will not be transmitted, because all the bandwidth will be occupied by audio.

Address

This parameter contains the IP address for the stream. If this field contains a unicast IP address, it will be automatically overwritten by the IP address of the system that has requested to view the stream from an HTML page supplied by an internal web server. By pressing the “Active” key on the configuration page, you can activate streaming: the system will start the transmission of audio and video packets to the selected IP address.

If the IP address is multicast, streaming will be sent to a multicast group identified directly by the IP address, enabling viewing by a large number of users (theoretically unlimited).

Port

This parameter contains the number of the UDP port where audio packets are to be sent. Since the streaming content is RTP, data are sent to four different ports: one port for audio, one port for video and two ports for the RTP information corresponding to both streams. Therefore, starting with an audio port number, it is implied that the audio data will be sent to this port number, video data will be sent to the audio port number plus two, and the odd port numbers before and after the video port will be used for RTP data. For example, if the audio port number is 554, the port number for video will be 556, and the port numbers for RTP data on both streams will be 555 and 557.

TTL/Hops

This parameter contains the value for the Time to Live associated with multicast packets.

Activate

Streaming activation/deactivation request.

Viewing with a plug-in

The integrated Web Server provides the simplest method.

Connect to the System via the Web and from the server homepage click on the image that looks like video—this will give you access to the page produced by streaming. This page has been designed to use Quick Time, which must have been previously installed to view the video stream. Accessing the page automatically activates audio-video streaming. The user can choose the video signal to be displayed (Local or Automatic), which must be compatible with configured settings. The System provides a direct link to streaming page, using the address: <http://aaa.bbb.ccc.ddd/streamviewen.asp>, where aaa.bbb.ccc.ddd is the IP address of the System.

Viewing using an external player

Another way of viewing streaming is to use an external player. The only tested players are QuickTime 6.0 and VIC (supplied by the University of California Berkeley), but this does not exclude the possibility of compatibility with other players that accept RTP streams.

The first operation necessary is to activate streaming. This can be achieved by simply entering the IP address of the system in the “Address” field on the streaming configuration page of the system where the player is located, or the multicast address of the group to whom the stream is being sent. Pressing the “Activate” key will enable the machine to begin the transmission of audio-video packets to the player.

If you use QuickTime as a player, you can simply select “File” from the menu, then “Open URL in new player” and enter `http://aaa.bbb.ccc.ddd/stream.sdp` where `aaa.bbb.ccc.ddd` is the IP address of the System that is to send the stream.

Viewing using a Distribution Server

Distribution servers offer a range of services for stream management that the System cannot offer directly. If users would like to make use of a distribution server for streaming transmission sent from a System, they can do so in accordance with the server’s characteristics.

Using a Proxy

Multicast streaming transmissions require an appropriate network configuration, with limitations imposed by the presence of any Firewall or Proxy. To offer good protection, these must block IP packets directed to unknown ports, such as the UDP ports used for audio and video streams. If the stream has to pass through such equipment, the equipment must be configured for any eventual multicast and have the appropriate ports enabled for streaming.

If the stream is sent over an internal network, problems can still arise if it is necessary to pass through a firewall in order to gain external access.

Deactivate Streaming

In order to stop streaming, go to the “Deactivate” key on the streaming configuration page and press OK, or simply close the browser.

PPPoE

(Point-to-Point Protocol over Ethernet)

PPPoE is used to allow Internet Service Providers (ISPs) to use their existing Radius (*) authentication systems from dialup services on broadband/Ethernet-based services.

“Automatic IP address”: If selected, an automatic IP address will be assigned.

- IP address: Enter static IP address provided by the ISP
- Subnet Mask: Enter subnet mask provided by the ISP.
- DNS Server IP address: Enter DNS server address provided by the ISP.

“Advanced”

This section contains configuration parameters, assigned by the ISP.

Once **“PPPoE active”** is selected, enter following data:

- User name: user name assigned by the ISP.
- Password: password assigned by the ISP.
- Server name: ISP server name.
- Service Name: Default (field empty).
Alpha numeric string for remote control of equipment connected with PPPoE server (ex. modem).
- **Connection mode**
Two different WAN connection modes are available:
 - Always connected
 - On call

“Bandwidth”

By selecting the “BANDWIDTH” icon, it is possible to enable and set maximum bandwidth usage limits (in Kbps). These limits can be different in transmission and reception, a very useful function for ADSL networks.

On the PPPoE configuration page there is a **PPPoE status LED**:

White: service not enabled

Red: service enabled, but not active

Green: service enabled and active

Enable network

It is possible to enable/disable any calling protocol.

Once explicitly disabled, a protocol will no longer appear in the “combo-box” for call selection. An incoming call will be always accepted, even if the incoming protocol is disabled.

* Radius: Remote Authentication Dial-In User Service

Location

From the “Home Page” select:

1. SETTINGS
2. INSTALLATION
3. LOCATION.

The following page will be displayed:



This section contains regional data about the terminal:

Terminal Name: Enter a name for the terminal

Country Name: Select the country. An international country code will be automatically provided.

Language: Select the desired language.

PBX: Enter the PBX access number for an outgoing call.

Audio Coding: Select the type of audio encoding in “Transmission.”

Video Standard: Select the video standard (PAL/NTSC), depending on the peripheral connected to Video Out.

Selection Tone: Select the desired tone.

Camera Frequency: <Auto> or 50Hz (NTSC).

Load default settings

From the “Home Page” select:

1. SETTINGS
2. INSTALLATION

From here, the default System configuration can be reloaded.

There are two options:

- “User settings only”
- “Factory Defaults”.

Once selected the desired option from the dropdown menu, move to the “LOAD DEFAULT VALUES” icon and press OK.

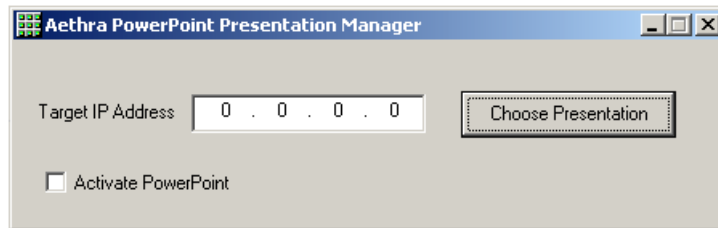
Read all instructions carefully.

If the “FACTORY SETTINGS” option has been chosen, users will be asked, as a precaution, for confirmation. An affirmative answer will result in the factory settings being reloaded. All user settings and data will be lost, including call history, phonebook numbers and static IP addresses.

Presentations

During a call, the system allows to send slides or still images in Jpeg format that have been previously loaded on the system using a PC.




- To load files onto the system, a PC with the AePPTManager program installed must be used. The program can be downloaded by entering the System WEB interface and selecting the “TOOLS” icon.
 1. Download the AePPTManager.exe software
 2. Start AePPTManager.exe
 3. For a correct operation, files must be extract to a PC folder.
 4. The self-extracting file includes AePPTManager.exe and AePPTManager.ini.
- Executing the program will display the following:



1. The program requests you to enter the system’s IP address and to choose the presentation to transfer.
2. By pressing the SLIDE key on the remote control, you will enter the presentation manager page.



3. Selecting the “DISPLAY PRESENTATIONS” icon and pressing OK will cause the first nine slides of the presentation being displayed on video.
4. You can select a slide by moving the remote control arrows and pressing OK. The slide will be locally displayed at full-screen and sent to the remote system.
5. The presentation can be managed using the remote control arrows or using the icons that appear in the lower area of the screen.

	Go back to previous slide.
	Go to next slide.
	Show slide sequence.

To leave the presentation, press the HOME key on the remote control.

Slides storage

During a call, the system automatically stores slides or Jpeg images received from the remote system. Up to 50 images will be stored in a circular buffer, till the connection is terminated.

Slides recall via WEB client

Enter the System WEB interface, select “Camera and Video Control” and in the dialog box labelled “Photo” click “Photo Download.”

A list will be opened, containing slides named SnapshotXX.jpg.

Saving slides on a PC

When a file is selected, the image will be uploaded to the PC and shown by the browser. Do not forget to save it on the PC.

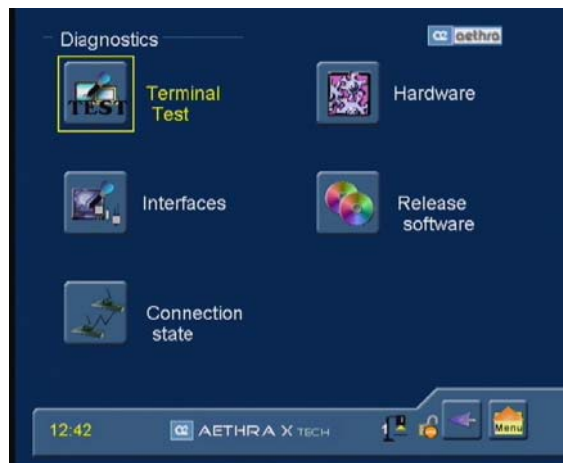
System Diagnostics

The System’s diagnostics menu allows you to perform tests and checks to verify that the system is properly working.

From the Home Page select:

1. SETTINGS
2. DIAGNOSTICS

The following page will be displayed:



Terminal test

This option performs an internal test of the system.

The test can be useful to diagnose audio/video problems encountered during a call. The test uses encoded local audio and video to simulate a connection. Press any keys to stop the test.

Interfaces

This option performs an internal test of the following interfaces:

- “Audio”.
For each input and output, peak values, noise and status can be visualized by means of graphical view-meters; in addition, the transmission and reception streams can be seen. Finally, it is possible to generate a tone (Tone Loc.) to test the speaker volume, and the selection of “Tx Tone” during a connection will generate an audible tone at the remote system.
- “Video”.
In this section you can view information on the active video input type and the video standard in use.
- “Network”.
In this menu you can view information about the detected interfaces
For ISDN accesses an LED status indicator is available:
Red – BRI access is disabled or in error.
Yellow – BRI access is functioning, but Level 1 is not active.
Green – Level 1 is active.

Connection Status

This section contains information about call status, including parameters such as incoming and outgoing audio and video bandwidth, incoming and outgoing video frame rates, and protocols in use.

The “Connection status” page is displayed in a window overlaid on the current video. The “CANCEL” key on the remote control can be used to change the transparency. To move within the table, press the “OK” key, then use the up and down arrows keys to navigate. To exit the page, press the left arrow keys.

ISDN

In an ISDN call, you can check certain data about the connection: rate, audio encoding, video encoding, frames/sec., and status of data channels.

In addition, by going to the “Accesses” icon and pressing OK, you can enter a page of advanced diagnostics, used to monitor in greater detail the state of individual ISDN accesses.

For each access you can see whether it is configured or not, whether it is active or not, and for each single access channel you can gain information such as the state, the number, cause of disconnection, “Error H.221” messages, and the delay.

IP

For IP calls, you can check certain data related to the Audio and Video IP connection: bit rate, audio and video encoding types, frames/packets (for audio), frames/sec. (for video), and number of lost packets.

Hardware

This section contains basic hardware information such as internal temperature and MAC address. Information about the processor and audio/video system can also be found in the Audio and Video submenus.

Software Versions

This section shows contains information about the software modules installed on the system, including versions, build dates, etc.

Connecting a personal computer

The System can be connected to a personal computer either directly or via a network (LAN) in order to update software, change remote settings or perform diagnostic tests.

Connecting a PC to the System without LAN

To connect the System to a personal computer not connected to a LAN:

1. Connect an Ethernet cable to the System connector and to the network interface card of your PC.
2. From the home page, navigate through the following menus:
 - Home Page
 - SETTINGS
 - INSTALLATION
 - NETWORK INTERFACES
 - IP
 - IP CONFIGURATION
 - IP CONFIGURATION

Ensure that the System belongs to the same subnet as the PC, but has a different address. If this is not true, change the System's IP address and restart the system.

3. Start the browser on your PC. In the address bar, enter the System's IP address. The web page manager will appear.

Connecting to the System via a PC in a LAN

To connect to the System from a PC in a LAN:

1. Ensure that a LAN cable connects the System's rear connector to your LAN. The PC can be connected to a LAN node or to the LAN OUT connector at the rear of the System.
2. Switch on the System.
3. Navigate through the following menus:
 - Home Page
 - SETTINGS
 - INSTALLTION
 - NETWORK INTERFACES
 - IP
 - IP CONFIGURATION
 - IP CONFIGURATION
4. If your LAN does not use a DHCP server, leave the Automatic IP Address box unchecked and enter the IP Address, the SubNet mask, Gateway IP Address and the DNS Server IP Address supplied by the network administrator, then restart the System.
5. On the PC, start Internet Explorer. Enter the System's IP address in the address bar of the browser.
6. The web page manager will appear.

Remote management

The System incorporates an integrated network server that allows management of the unit from a remote PC. Through this interface it is possible to:

- Execute diagnostic tests.
- Check a system.
- Change System settings.

Access to the web page

Start a web browser on your PC. Enter the System's IP address in the address bar of the browser. A request to enter the network password will be displayed. Always enter "Aethra" in the User Name field. The password can be changed from the default of "1234" in the system configuration menu.

1. Home Page
2. SETTINGS
3. INSTALLATION
4. NETWORK INTERFACES
5. IP
6. SERVICES
7. Web – Telnet Management

Note

The default Password is 1234.

For correct web page viewing in Windows Server 2003 you will need to activate script execution in Internet Explorer by selecting:

Tools / Internet Options / Security / Custom level / Scripting / Active scripting / Enable.


A page very similar to the System user interface Home page will be displayed. From here, you can make a call in the way previously described. The arrangement of the menus for configuration and diagnostics is also the same.

In addition to the normal menus, a TOOLS section has been added where the following downloads are available:

- The program DataConf.exe enables you to use NetMeeting 3.xx with ISDN or IP calls for multimedia activities (data channels T.120). See section "Managing the Data Conference Software".
- The program AePPTManager.exe enables you to load a PowerPoint presentation in the system.
- The file NoteB.dat enables you to save all the phonebook data(MCU excluded), and can also be used to transfer the data between systems.
- The file NoteBm.dat enables you to save all the phonebook data, and can also be used to transfer the data between systems.
- Finally, a module is present that enables you to update the System phonebook data, using files that are compatible with Aethra's proprietary phonebook format.

From the Home Page, click on TOOLS to access these options.

The language of the web interface can be toggled between English and Italian by clicking on the flag displayed at the top centre of the Home Page.

When using the web-based management features, use the  icon present on all pages to save changes.

Updating software

1. Download the update to a folder on a connected PC.
2. When executed, the program will display the following:



3. Enter the IP address of the system to be updated in the field labelled “Host IP Address.”
4. Press Start to begin the download.



Attention: During this procedure, follow the instructions displayed on the monitor. The download process requires a few minutes to complete. When the download has finished, the system will restart automatically.

Data Conference with Microsoft NetMeeting 3.xx

The Data Conference software that has been introduced is compatible with version 3.xx of Microsoft NetMeeting and allows you to connect via a LAN the System to a PC hosting NetMeeting.

This enables a user on a local network to exploit the System as a kind of bridge in order to manage T.120 videoconference data traffic on ISDN, LAN or NIC.

Download Data Conference

The file DataConf.exe is available for download on System web page, in the TOOLS section described above.



It is important to download the file DataConf.ini as well. This enables automatic configuration of the previous program and must be installed in the same folder where the DataConf.exe file was saved.

1. Download the software DataConf.exe;
2. Will be downloaded dc.exe file, start the file.
3. Download the software DataConf.ini
4. Start DataConf.exe.

Use of Data Conference

In order to use the System as a bridge for data transfer, navigate through the system menus as shown:

1. Home Page
2. SETTINGS
3. AUDIO – VIDEO – DATA
4. DATA CHANNEL

Configure this section as illustrated:

1. Data Channel: YES
2. Modem: NO
3. MLP: T.120
4. Serial Rate: 115200

For uses over LAN, go to the following sections:

1. Home Page
2. SETTINGS
3. INSTALLATION
4. NETWORK INTERFACE
5. IP
6. H.323 SETTINGS

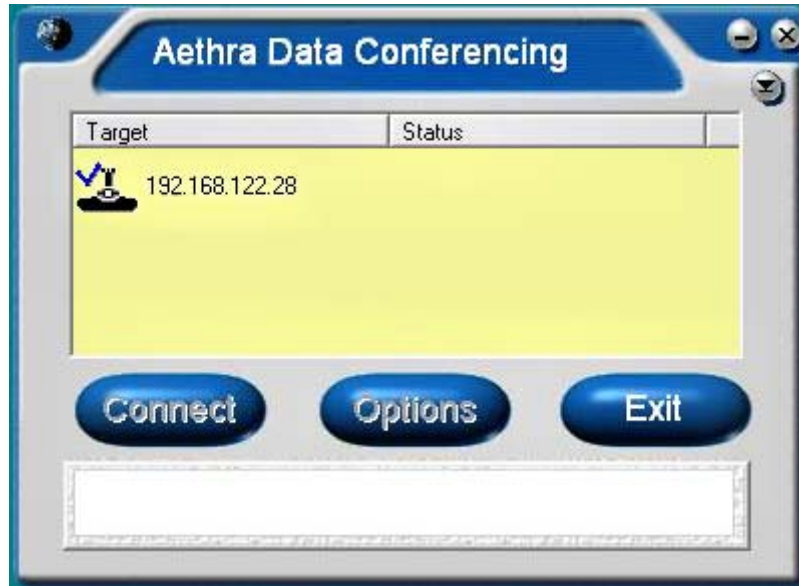
At this stage:

1. Check the box “Use NetMeeting”
2. Enter the IP address of the PC hosting NetMeeting.

Managing the DataConference software

Data Conference is typically used when two ISDN or LAN connected users decide to start a conference using T.120 communication.

Start the DataConf.exe program.



The program creates an automatic connection between the System and the PC. At this point, several items of information concerning the connection are displayed:

- The System IP address.
- The network interface used for video calls.
- The type of call: incoming or outgoing.
- The T.120 data channel active.
- The status of the NetMeeting connection between the two users.

Once the connection has been established, NetMeeting 3.xx is displayed in the foreground and you can perform all data conference management operations.

If you desire to change the IP address of the System, you have to disconnect, press the key "Configure" and enter the new address to use.

Appendices

Network Requirements IP\H.323

The network requirements for point-point connections between videoconferencing terminals are as follows.

The complete network path connecting two H.323 terminals must have a constant available bandwidth for the whole duration of the connection. The effective bandwidth used on LAN/WAN Full-Duplex network connections is equal to the sum of the Audio Rate and Video Rate, plus approximately 20% for TCP/IP overhead.

In the case of Half-Duplex LAN/WAN networks, the aforementioned bandwidth is doubled. For example, if it is necessary to guarantee a 384K connection for the video and a 64K for the audio, the bandwidth allocated must be at least $(384+64) * 1.2 \approx 540K$ for each Half-Duplex connection. In case of dial-up WAN links, it should be underlined that their efficiency in terms of “useful” bandwidth is approximately half the total available bandwidth.

It is always preferable to use mechanisms such as QoS for WANs because they take into account the total bandwidth required for a videoconference, rather than relying exclusively on over-dimensioning the network. This is necessary for the handling of increasing numbers of simultaneous connections or a network that is already loaded.

The network needs to be set up so that latency and jitter are as low as possible. Extended times for latency and variable jitter can create serious problems, especially in video quality.

It is always preferable for H.323 terminals to be connected to switched type LAN connections to avoid the traffic generated by terminals being superposed on the normal traffic present on the network.

It is preferable to avoid using NAT-type protocols on router interfaces that route H.323 packets, since NAT protocols often do not allow the correct routing of connections.

If NAT, firewall or access list implementations are to be used, they must be H.323 compatible.

NAT – FIREWALL Interoperability

Introduction

There are many strategic advantages for companies that succeed in making all traffic converge from voice applications, video and data to one IP network infrastructure.

Unfortunately, the drive to concentrate all IP communications onto one single network has reduced. The connection between a company’s corporate network and the Internet world is accomplished with firewalls and devices using NAT (Network Address Translation), which block voice and video calls via IP. Firewalls block IP traffic for video and voice by preventing any unsolicited communication from the outside. Devices implementing NAT block IP traffic because all equipment on the internal network uses private IP addresses, and can therefore not be contacted from outside the local domain.

There are several solutions to the problem of getting IP communications past NAT and firewalls: bypassing the firewall or NAT device, upgrading the network infrastructure with an Application Level Gateway (ALG), and going out through the firewall or NAT using semi-tunnelling connections.

Going around the firewall or NAT device is not the best solution for most companies. Removing the firewall or placing videoconferencing equipment on an unshielded section of the network could seriously compromise the network’s security.

Using these devices is very expensive and besides this an access policy for Firewalls and NATs would be needed. These devices should be located along the communication path at every point where a NAT and Firewall are present.

A second solution is the improvement of the network by the introduction of an ALG, but this is intrusive and potentially expensive. ALGs are software packages specifically designed for firewalls from various producers that examine every packet attempting to pass through the firewall in order to determine whether it concerns a known protocol like H.323 or SIP. If the packet contains a known protocol, the Firewall allows it through. However, like Proxies and MCUs that go around firewalls, ALGs also need an access policy for firewalls and every firewall or NAT device needs up-to-date ALG software. Because new protocols are continually being developed, ALG software must be updated frequently.

IP Voice and Video Crossing NAT and Firewall

The use of existing network infrastructures for the transmission of voice, video and data promises interesting strategic advantages for companies of all sizes. Commonly known as “rich media communications” or “Internet Protocol (IP) communications” these technologies for converging networks offer new opportunities to communicate, coordinate and collaborate with customers, suppliers, commercial partners and others all over the world.

Unfortunately, the protocols used for IP communications conflict with most of the security mechanisms for networks (such as Firewalls and NAT), resulting in protracted or late implementation times for IP video and voice applications.

Firewalls and NATs – How they work

In an IP network, every device is assigned a unique IP address. All computers, telephones, and videoconference terminals have at their disposal approximately 65,000 ports for the purpose of establishing communication channels to transmit data to other devices on the network.

Messages between IP network devices are composed of packets that contain the following information: the IP address of the terminal that has generated the message, the port number from which the message has been sent, the IP address of the destination terminal, the port number at the destination, and the data being sent.

Firewalls

Companies that allow connection to the Internet by their employees typically install a firewall in order to prevent external access of or tampering with internal data.

The firewall examines the destination IP address and port number of every packet received from outside. Usually, firewalls are configured in such a way that if a computer from inside the firewall requests data from a computer outside the firewall, the response packets will be allowed through from the external computer, but only if they are sent to the IP address and port of the internal computer that generated the request.

If the Firewall receives a packet destined for a computer that is located internally and determines that the destination computer has not initiated any communication, the firewall discards the incoming packet.

Firewalls are nearly always configured to block all incoming traffic that has not been explicitly requested. Internal web servers are the exception: they must be accessible from the outside. To allow this, the network administrator configures the Firewall to let through packets destined for port 80 of the IP address of the web server. This operation allows external users to send requests to connect to the company’s web server in order to access data on that server.

NAT (Network Address Translation)

Network Address Translation is an Internet standard that allows a LAN (Local Area Network) to use a set of IP addresses for internal traffic and another address (or set of addresses) to connect to services on an external network (the internet, for example). Devices that implement NAT are located at boundaries between the LAN and the external network, and their purpose is to provide translation of IP addresses for all packets that are destined for the external network. Many organisations use NAT as a security mechanism because it masks the internal IP addresses—if hackers do not know the IP address of a machine, they cannot attack it and cause disruptions. NAT also allows a company to use more IP addresses than they might otherwise be allocated. Since these addresses are only used internally, there is no problem with IP address conflicts with other organisations.

Problems with Video and Voice Communications on NAT/Firewall Protected Networks

The IP based voice and video protocols like H.323 require that terminals be capable of establishing audio-video communication channels using IP addresses and data ports. In this situation, a problem arises: terminals must “listen” for incoming calls to establish IP connections, but the firewall is generally configured in such a way as not to allow packets past that are not expressly requested. Even if the network administrator left a port open for the terminal to receive notification of a call (port 1720, designated as a “well-known TCP port”) the video and voice communication protocols for IP necessitate the opening of other ports in order to receive control messages and open audio and video channels.

The identities of these additional ports are determined dynamically, not in advance, meaning that the network administrator would have to open all the firewall ports to allow video and voice communication, thus virtually disabling the firewall. Network administrators are unlikely to do this (and wisely so), since it effectively eliminates network security policies. NAT also creates an obstacle for voice and video communications over IP. NAT allows an organisation to assign private IP addresses to machines on the local network, but routers that control the flow of data towards the internet can handle only packets with routable addresses or public IP addresses.

A terminal located behind the NAT device on the LAN can initiate communication with any other terminal in the same LAN because the IP addresses within the LAN are routable, meaning that it is possible to have subnets in a company managed by an internal router. This allows the establishment of audio-video communications on different branches of the subnet.

Because they have private addresses, and are therefore not accessible from outside the NAT, terminals on the LAN cannot be reached by externally originating calls. Even if they initiate calls to external terminals, a problem still arises. When the call is initiated, the IP address of the calling terminal is contained in the payload of the packet sent. The destination terminal receives call setup packets, examines them and starts to transmit audio and video towards the terminal from which the call was received, and from which the IP address was obtained by examining the contents of the received packets.

If this IP address is private, the router for Internet access discards the audio and video packets sent from the terminal external to NAT towards the internal terminal because the packets sent were non-routable. The connection between two terminals appears to be successful but in reality the NAT-internal terminal never receives the audio or video from the external terminal.

Solution for the NAT/Firewall Problem

The only equipment that does not create any of the problems described above is a NAT/firewall H.323-compatible device. Such a firewall does not block the TCP 1720 port and allows access to the other, dynamically-determined H.323 ports.

Videoconferencing systems usually have private IP addresses that are not accessible from external routers. To allow calls to function properly, the network administrator can define static NAT (a

permanent association between a private IP address and a public IP address reserved for H.323 videoconferences) for every terminal that must be accessible from an external connection. The NAT device substitutes the static IP address in the payload and header setup packet sent from the internal terminal to the external terminal. The destination terminal uses that address for addressing the reply packets, which are routed through the NAT device to the internal terminal.

Firewall ALG

Application Level Gateways (ALGs) are firewalls programmed to recognize specific IP protocols like H.323.

Instead of looking only at the information contained in packet headers to determine whether to transmit or block packets, ALGs analyse in detail the data contained in the payload packet. The H.323 protocol inserts important control information such as audio and video port identification in the payload packets. The terminal expects to receive audio and video connections from the remote calling terminal on these ports. By analysing which port the terminal expects to use, the ALG dynamically opens only those ports, leaving the others closed to preserve network security. An example of a firewall ALG follows.

The Aethra Application Level Gateway is present in the Aethra Stargate xDSL Router and allows any videoconferencing terminal, independent of its manufacturer, resolve the NAT/firewall problem. The Stargate router is capable of checking every incoming and outgoing H.323 call and dynamically opening only the ports being used for the H.323 videoconference.

The Stargate router also supports NAT functionality and is therefore capable of substituting the public NAT address for the private IP address automatically inserted in the H.323 payload packets by the internal terminal. When the Aethra ALG functionality is used with an Aethra videoconferencing system, the “Aethra NAT” function of the videoconferencing system must be disabled because the network equipment is H.323 compatible.

Technical specifics

Supported Standards

- ITU-T H.320 ISDN, leased networks
- ITU-T H.323 IP networks
- IETF-SIP (RFC3261) IP networks
- PPoE
- Video H.261, H.263++, H.264 H.239, H.241
- Audio G.711, G.728, G.722, G.722.1, MPEG4 AAC-LD
- Data T.120
- LDAP H.350
- MCU compatibility H.243, H.231

Transmission

- Bit rate 56 kbps ÷ 128 kbps over ISDN BRI 64 kbps ÷ 2 Mbps over IP (H323/SIP), Asymmetric rates
- Simultaneous video motion coding and PC presentations from the DVI/XGA input

Video

- Frame rate 15 frames per second @ 56 kbps - 128 kbps 30 frames per second @ 168 kbps - 2 Mbps
- Video resolution 4CIF 704 x 576 pixels FCIF 352 x 288 pixels QCIF 176 x 144 pixels 4CIF 704 x 576 pixels for still images (H.261 Annex D) Up to 1024 x 768 over XGA in H.263
- Remote camera control H.281 (H.320 - H.323)

Audio

- | Audio | Band | Bit rate |
|---------|---------------|---------------|
| G.711 | 300 ÷ 3400 Hz | 56 kbps |
| G.728 | 50 ÷ 3400 Hz | 16 kbps |
| G.722 | 50 ÷ 7000 Hz | 48/56 kbps |
| G.722.1 | 50 ÷ 7000 Hz | 24/32 kbps |
| AAC-LD | 50 ÷ 14000 Hz | 48/56/64 kbps |
- Echo cancellation Full-duplex
 - Adaptive post filtering
 - Automatic Gain Control (AGC)
 - Automatic Noise Suppression

Digital Microphone Pod

- Range Cardioid
- Response 50 ÷ 14000 Hz
- Microphones 1
- Mute button

Built-in Camera

- Resolution 752 x 582 pixels
- Presets 122 presets
- H. angle of view 6.6 to 65 degrees
- Zoom 40x (10x optical + 4x digital)

Supported Monitor

- Format PAL or NTSC or VGA
- Single, dual monitor, VGA
- PiP function
- 16:9 support
- Dual Monitor Emulation

Network Interfaces

- Basic version ISDN 1 BRI with integrated channel aggregator 1 RJ-45 Ethernet 2-Port 10/100BASE-T full-duplex with integrated switch Ethernet 2 RJ-45
- Optional Embedded WiFi IEEE 802.11b/g

Audio/Video Interfaces

- Video inputs Main camera Integrated Y/C, not accessible Composite (RCA) Aux Composite (RCA) XGA In DVI_I
- Video outputs Monitor Composite (RCA) XGA Out DVI_I
- Audio inputs Connection Level Connector Pod mic. 360° Dig. RJ-11 6/6 Aux. mic. Mic Stereo jack 3.5 mm Audio In Line RCA
- Audio outputs Connection Level Connector Monitor Line RCA Aux Line Stereo jack 3.5 mm

Auxiliary Interfaces

- Data & Diagnostics RS232 Mini-DIN 8-pin with DB9 adapter
- VISCA RS232 Mini-DIN 8-pin supports Canon or Sony, aux PTZ camera

User Interface

- Multilingual on-screen graphic user interface
- User selectable languages: Italian, English, French, Spanish, German, Portuguese, Norwegian, Swedish, Russian, Czechoslovakian, Hungarian, Chinese, Japanese, Korean
- Infrared remote control for full function control
- Contextual help
- Diagnostics and management functions
- Call progress monitoring
- Supports AMX™ or Crestron™
- Customizable Graphic User Interface

Encryption

- AES encryption standard H.233, H.234, H.235

Web Management

All the configuration, call, diagnostics and management functions are accessible using the following web browsers: Microsoft® Internet Explorer®, Netscape Navigator®

Remote Diagnostics and Management

	Local	Web Browser	SNMP
Self test	Yes	Yes	Yes
Diagnostics	Yes	Yes	Yes
Configuration	Yes	Yes	Yes
Call	Yes	Yes	
Error tracking	Yes	Yes	Yes

Integrated Presentation

- Supported applications Microsoft® PowerPoint®
- Multimedia support T.120

Power Supply

- 100-240 Vac 50-60 Hz 1.5 A Max

Dimensions

- VEGA X3 Width 30 cm (11.8") Height 14 cm (5.5") Depth 20.5 cm (8")

Troubleshooting Problems

PROBLEM	SOLUTION
Nothing displayed on monitor.	Check that the System is switched on. Check that the System monitor is on by pushing the on/off key at the front of the monitor. If the problem persists, contact the Aethra Help Desk.
I see no video camera signal in Self View and the picture is dark.	Check that the integrated video camera has no objects obscuring the lens. Select as the input the video camera called “Room” using either the remote control or the web interface. If the problem persists, contact the Aethra Help Desk.
No audio transmitted.	Check that there are no objects close to the microphone. Use the integrated diagnostics (see related manual section). If the problem persists, contact the Aethra Help Desk.
The LAN lamp (LED) is flashing, but I cannot successfully PING the system.	Check that the system’s IP address is not duplicated in the network. If the problem persists, contact the Aethra Help Desk.
I cannot establish a data connection between the two systems.	Check that the data channel is enabled (see related section in this manual). Check that the IP of the DataConf is the same as that of the system to be connected. If the connection is IP, make sure that the check box “Use NetMeeting” is checked and the PC IP address to be connected is correct (see relevant section in this manual). If the problem persists, contact the Aethra Help Desk.
I cannot make an IP connection and my IP address is correct.	Check that the system is switched on. Check that the system can be reached using PING. Check that the Gatekeeper for both systems is enabled/disabled. If the problem persists, contact the Aethra Help Desk.
The Self View picture is black and white and is rolling from bottom to top.	Check that the video-standard used (NTSC or PAL) is correctly selected in the menu: INSTALLATION → LOCATION
The picture transmitted from my equipment is too dark.	Ensure that the video camera is not pointing at a luminous source (neon light, window etc.).
Audio received is unclear and you only hear the audio in bursts.	Place the integrated microphone farther away from any speakers (TV, system speakers etc.). Ensure that the volume is not too high and that echo cancellation is activated.

Glossary

AACLD Advanced Audio Coding Low Delay	PAL Phase Alternation Line
AES Advanced Encryption Standard	PBX Private Branch Exchange
AGC : Automatic Gain Control.	PC Personal Computer
BRI Basic Rate Interface	PiP Picture-In-Picture
CD Collision Detection	PRI Primary Rate Interface
CE Communittee European	QCIF Quarter Common Intermediate Format
CIF Common Intermediate Format	QoS Quality of Service
CLIR Calling Line Identity Restriction	Router A device that attaches two or more network devices and forwards data accordingly.
CODEC Coder/Decoder	RTS Ready To Send
COLR Connected Line Identity Restriction	SIF Source Input Format
CRC Cyclic Redundancy Checking	SNMP Simple Network Management Protocol
CSU Channel Service Unit	SPID Service Provider Identification
CTS Clear To Send	SQCIF Sub-Quarter Common Intermediate Format
DHCP Dynamic Host Configuration Protocol	SVGA Super Video Graphics Array
DTR Data Transfer Rate	TCP/IP Trasmission Control Protocol/Internet Protocol
DVI (-I) Digital Video Interface (integrated)	TCS Terminal Control String
IEC International Electrotechnical Commission	TOS Type Of Service
IP Address Internet Protocol Address	TTL Time To Live
ISDN Integrate Services Digital Network	UDP User Datagram Protocol
ISP Internet Service Provider	UL Underwriters Laboratories
LAN Local Area Network	VCR Video Cassette Recorder
MCU Multi-point Control Unit	VGA Video Graphics Array
MIC Microphone	VISCA Video System Control Architecture
MSN Multiple Subscriber Number	VNC Virtual Network Computing
NAT Network Address translation	WAN Wide Area Network
NR Noise Reduction	XGA Extended Graphics Array
NSF Non Standard Facility	
NT Network Termination	
NTSC National Television Systems Committee	
PABX Private Automatic Branch Exchange	


USE AND STORAGE CONDITIONS

OPERATING TEMPERATURE	+0°C ÷ +40 °C
RELATIVE OPERATING HUMIDITY	10% ÷ 93 % (without condensation)
STORAGE TEMPERATURE	-40 ÷ +70 °C

REFERENCE REGULATIONS (CE MARK AND RELIABILITY TESTS)

STORAGE	EN 60068-2-1 Test Ab (IEC 60068-2-1) EN 60068-2-2 Test Bb (IEC 60068-2-2)
TRANSPORTATION	IEC 60068-2-32 Test Ed - Method 1 IEC 60068-2-64 Test Fdb (CEI 50-6/9)
OPERATING CONDITIONS	CEI 50-3 EN 60068-2-1 Test Ab (IEC 60068-2-1) EN 60068-2-2 Test Bb (IEC 60068-2-2) IEC 60068-2-14 Test Nb IEC 60068-2-56 Test Cb IEC 60068-2-6 Test Fc IEC 60068-2-31 Test Ec IEC 60068-2-32 Test Ed - Method 1 IEC 60068-2-64 Test Fdb (CEI 50-6/9)
EMC	EN 55022 EN 55024 EN 61000-3-2 EN 61000-3-3 FCC15 *
SAFETY	EN 60950-1 (IEC 60950-1)
CONNECTION TO TELECOMMUNICATION NETWORK	FCC 68 *

* Equipment for USA market only

	<p>Hereby, Aethra S.p.A. declares that this device complies with essential requirements and other relevant notes of R&TTE Directive 1999/5/EC.</p> <p>The declaration of conformity maybe obtained from: Aethra S.p.A. - Via Matteo Ricci, 10 - 60020 Ancona - Italy www.aethra.com info.aethra@aethra.com</p>
---	--