iPATH™ Agility Controller

iPATH Agility Controller manages your Agility network and its connected users.

This self-contained server unit contains all necessary hardware and software.

Customer Support Information

Order toll-free in the U.S. or for FREE technical support 24/7: Call 877-877-BBOX
(outside U.S. call 724-746-5500)
www.blackbox.com • info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

We're here to help! If you have any questions about your application
or our products, contact Black Box Tech Support at **877-877-2269**
or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 60 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad

(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio cAgilityicado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objetos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal cAgilityicado deberá ser provisto cuando:
    A: El cable de poder o el contacto ha sido dañado; u
    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    C: El aparato ha sido expuesto a la lluvia; o
    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Contents

1. Specifications

Approvals:	CE, FCC
Hardware Compatibility:	All computers via Agility units
Software Compatibility:	Operates with all known software and operating systems including Windows®, Linux®, Unix®, BSD, all Sun® OS, all Mac® OS, NetWare®, etc.

Connectors:	Video:	VGA female (used for showing current IP address only)
	Network:	2 x RJ45 Ethernet sockets
	Other:	Power jack

Operating Temperature:	32 to 104°F (0 to 40°C)

Power:	DC jack (power adapter included)	
	Input:	100–240 VAC, 50/60 Hz
	Output:	12VDC, 60W

Dimensions (w x h x d):	430mm (16.93") x 44.5mm (1.75") x 230mm (9.05")
Weights:	2.7kg (5.95lbs)

1.1 Lithium battery

CAUTION: This product contains a lithium battery which must be disposed of in the correct manner.

CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.

• If the lithium battery needs to be changed, you must return the product to your nearest Black Box dealer. The battery must be replaced by an authorized Black Box dealer.

• Once the product has come to the end of its useful life, the lithium battery must be removed as part of the decommissioning process and recycled in strict accordance with the regulations stipulated by your local authority. Advice on battery removal can be provided on request by Black Box.

2. Introduction

Black Box Agility local and remote units allow multiple remote users to access host computers in a very flexible manner. Such flexibility requires management and coordination – that is where the iPATH Agility Controller becomes vital.

iPATH Agility Controller is designed to promote the most efficient use of Agility units by allowing central control over any number of transmitters (more commonly referred to as 'Channels' within iPATH Agility Controller) and receivers. Using the intuitive iPATH Agility Controller web-based interface, one or more administrators can manage potentially thousands of users who are interacting with an almost unlimited number of devices.

iPATH Agility Controller operates from a self-contained compact server unit that can be situated anywhere within your network, as shown in Figure 2-1:
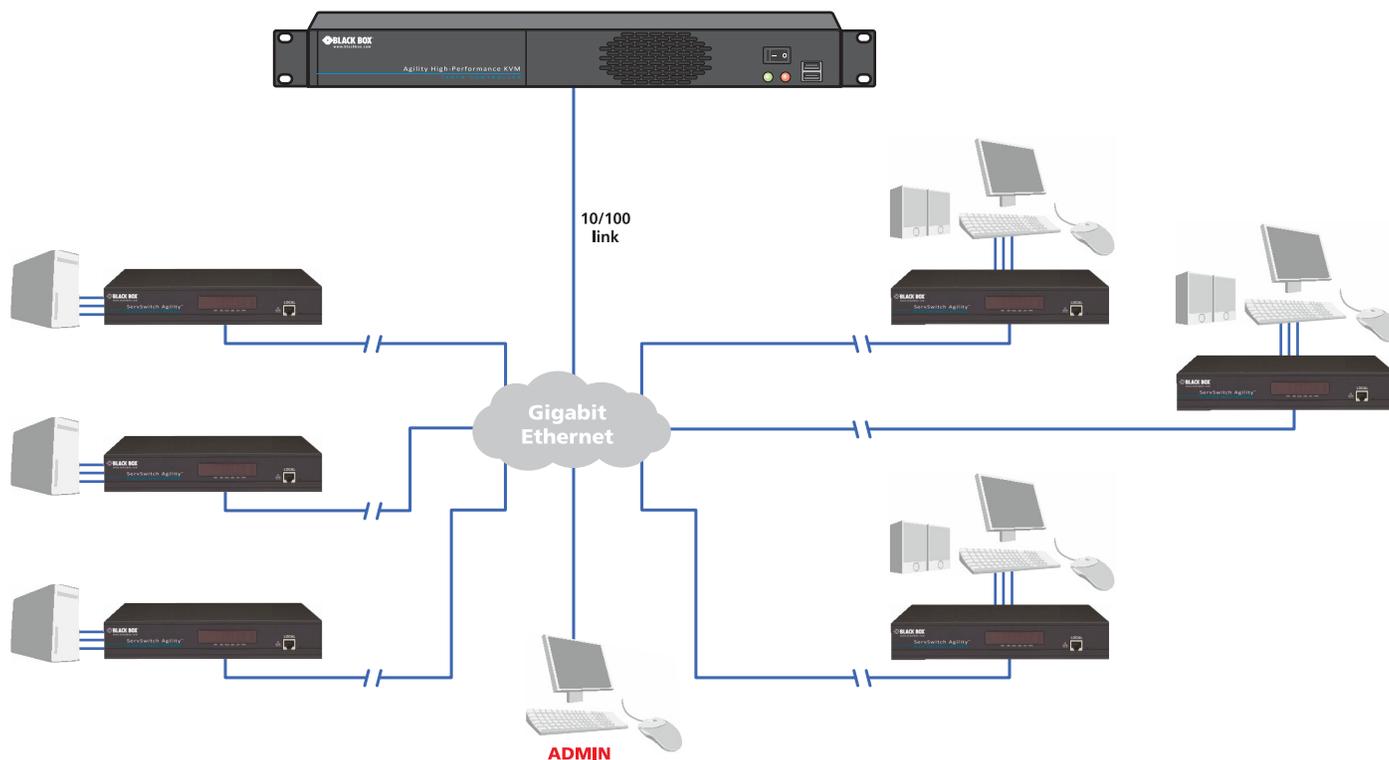
Figure 2-1. The iPATH Agility Controller connects to your network and provides administrative control over the various Agility transmitters, receivers and their users.

Note: Although the Agility units require Gigabit Ethernet connections, in its administrative role, the iPATH Agility Controller requires only a 10-/100-Mbps connection to the network.

The iPATH Agility Controller is supplied pre-loaded and is straightforward to deploy, requiring only a network connection and a power input to begin operation. All configuration of your Agility transmitters (channels), receivers and users are performed using the intuitive iPATH Agility Controller browser interface via a network connected computer.

2.1 Agility/iPATH features

2.1.1 AFZ lossless codec

The AFZ compression scheme is primarily focused on improving the performance for "natural" images (i.e. photographs and movies) and is automatically selected whenever there is a benefit to do so. The AFZ codec is lossless and is very low latency (a small fraction of a frame delay). It generally achieves 50% improvement (in compression) over the RLE scheme for any areas of the screen that consist of images, gradients, shadows etc., elements commonly found in modern desktop environments.

To maintain compatibility with non AFZ -enabled transmitters and receivers there is an automatic switching method which will revert back to RLE compression when a Agility R1 receiver is connected to the newer Agility R2 series or Agility Dual.

2.1.2 New feature: AFZ+ codec

AFZ+ compliments the existing AFZ codec by providing greater compression for increased speed where pixel perfect results are not the primary focus. The transmitter video configuration page allows you to choose the required compression mode. Choices are:

- 'Pixel perfect' - only uses pixel perfect AFZ,

- 'Adaptive' - guarantees frame rate, builds to pixel perfect,

- 'Smoothest video' - forces the maximum compression, or

- 'Advanced' - allows you to choose the mode:
  - 'AFZ only (pixel perfect),
  - 'AFZ+ Minimum compression',
  - 'AFZ+ Middle compression', or
  - 'AFZ+ Maximum compression'.

2.1.3 Magic Eye (anti-dither support added)

The Magic Eye feature increases performance and reduces network traffic when Agility units are used with Apple Macs and other host computers that have dithered video output. It also improves performance if the video source is noisy (e.g. from a VGA-to-DVI converter).

Dithering is a technique used by some graphics cards to improve perceived image quality by continuously varying the color of each pixel slightly. This gives the illusion of more shades of color than the display can really reproduce, and smooths the appearance of gradually shaded areas in images. Unfortunately dithering is an issue for KVM extenders such as Agility because it makes the image appear to be changing all the time even when it is static, thus creating much more network data than can be carried by a Gigabit Ethernet. The result is a reduction in video frame rate, which the user sees as slow mouse response.

Magic Eye works by ignoring small variations in the video from frame to frame. It is enabled by default as it is not obvious to the user that his poor mouse behavior is caused by dithering. In most cases Magic Eye is invisible, but it can produce slight color inaccuracies on the monitor. For full color accuracy, Magic Eye can be disabled (within the transmitter video configuration page) for video sources which are not dithered or noisy.

2.1.4 Transport Layer Security (TLS)

Agility and Agility Dual units support the industry standard Transport Layer Security (TLS) protocol. This offers protection against eavesdropping and tampering by third parties when data are transferred between Agility transmitters and receivers across networks (and also between Agility units and iPATH Agility Controllers).
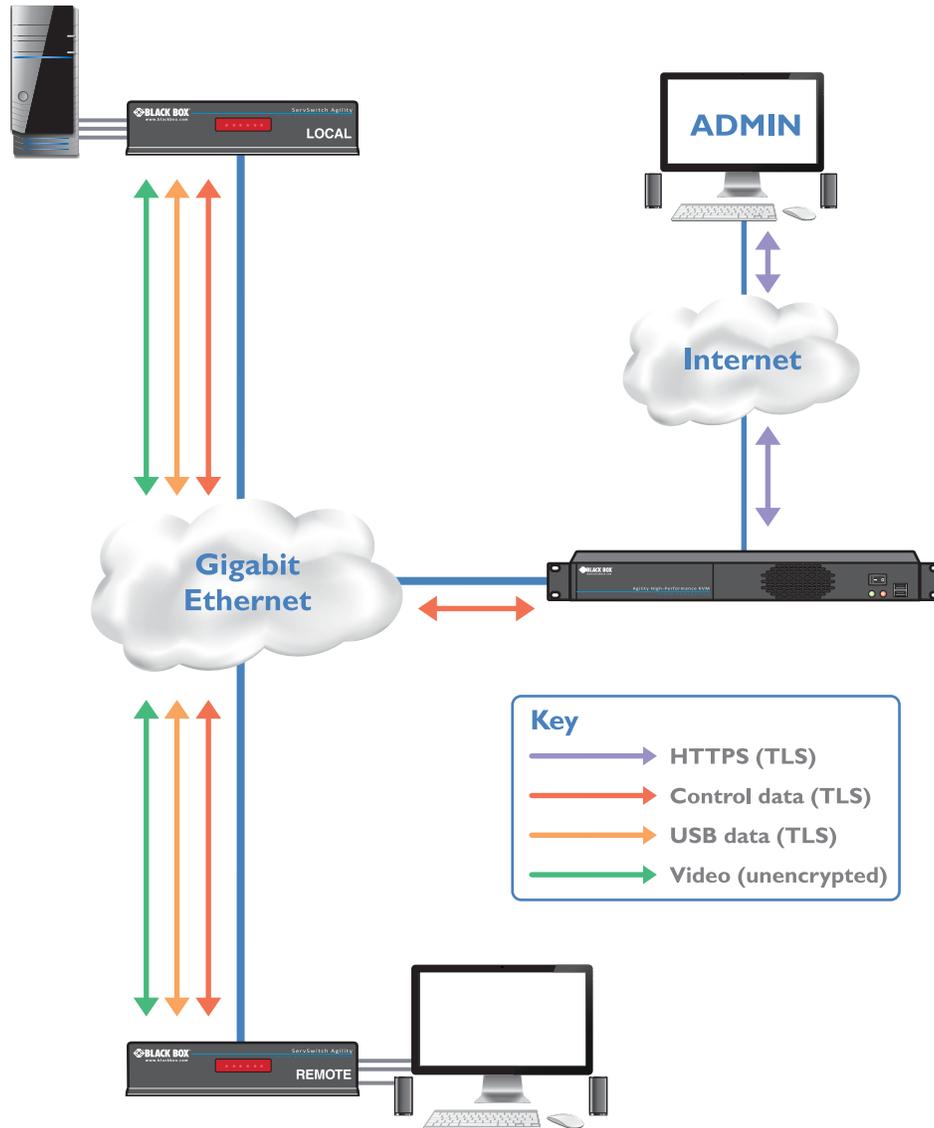
Figure 2-2. Transport Layer Security data diagram

2.2 Teaming operation

The units have dual network interface ports which can be used in parallel to produce important benefits:

• Improved connection speeds up to 2 Gigabits per second, and

• Important link redundancy that can maintain operation in the event of a failed connection.

Teaming offers immediate speed improvements in a one-to-one arrangement...

System Port link

Teaming Port link
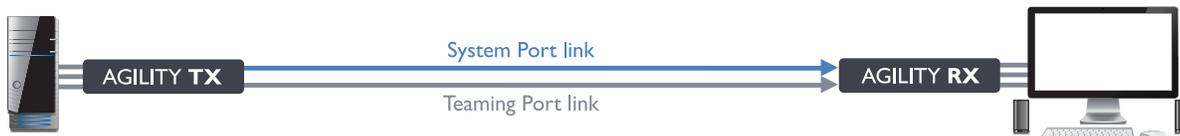
...and also in multicast installations:

System Port Multicast Group Addresses:
Video - **224.168.16.1**
Audio - **224.168.16.2**

Teaming Port Multicast Group Addresses:
Video - **224.168.16.11**
Audio - **224.168.16.12**
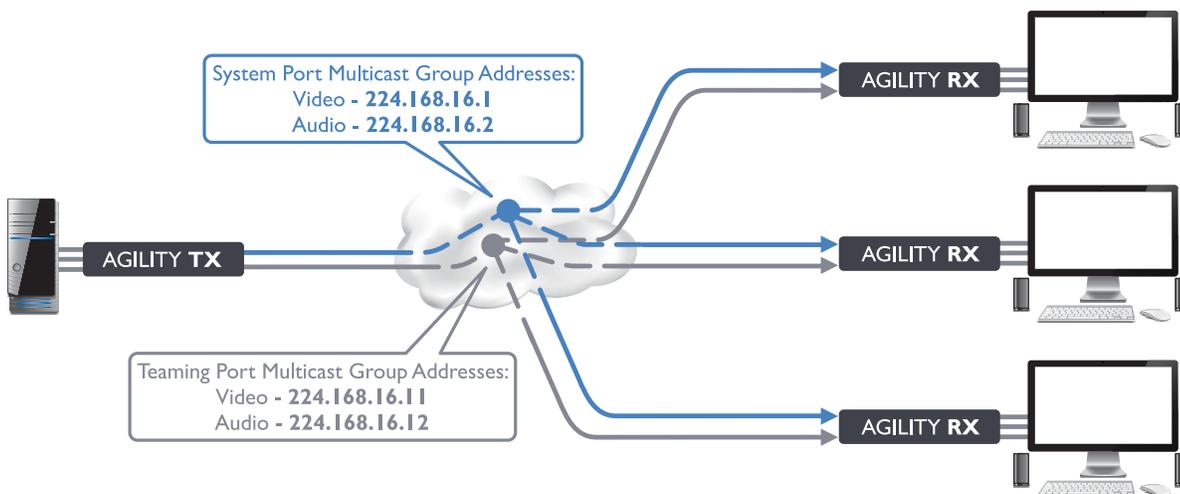
2.3 iPATH Agility Controller basics

2.3.1 Channels

Think of a channel as a 'virtual transmitter'. It is virtual because the video, audio and USB streams of a channel do not necessarily have to originate from the same physical transmitter unit, although in most cases they will. For instance, you could arrange for video and USB streams to be received from one host computer, while the audio stream came from an alternative source. Alternatively, two channels could be configured for the same host computer, each with different access rights to suit particular situations.

2.3.2 Groups

In order to accommodate potentially large numbers of users and devices, iPATH Agility Controller uses a system of groups: User Groups, Receiver Groups and Channel Groups. Groups allow the administrator to apply collective settings to all members and also to take full advantage of *Inheritance*. Inheritance allows members of a group to benefit from settings and permissions made within other groups to which their group is linked. This saves administration time because members do not need to be individually altered. For instance, if Sam is in User Group 1, all Channels accessible to User Group 1 will be available to Sam.

2.3.3 User Types

This guide refers to the two main categories of users involved with the iPATH Agility Controller system:

- An **Admin (administrator) user** accesses the iPATH Agility Controller system via a network-linked computer running an Internet browser. Once the necessary username and password have been entered, Admin users can make changes to the operation of the iPATH Agility Controller system.

- A **Regular user** has a keyboard, video monitor and mouse (plus speakers where appropriate) attached to a Agility receiver unit and can access one or more computers that are linked to Agility transmitters. The Agility receiver provides an On-Screen Display (OSD) that lists all accessible computers and allows easy access to them.

2.3.4 Security

Security considerations form a major part of iPATH Agility Controller operation, ensuring that users have rapid access only to the systems for which they have permission. At its core, iPATH Agility Controller manages an important three-way relationship between the users, the Agility receiver(s) and the channels from the host computers.

The diagram shows a representation of the three-way relationship which exists between users, receivers and channels, as shown in Figure 2-3:
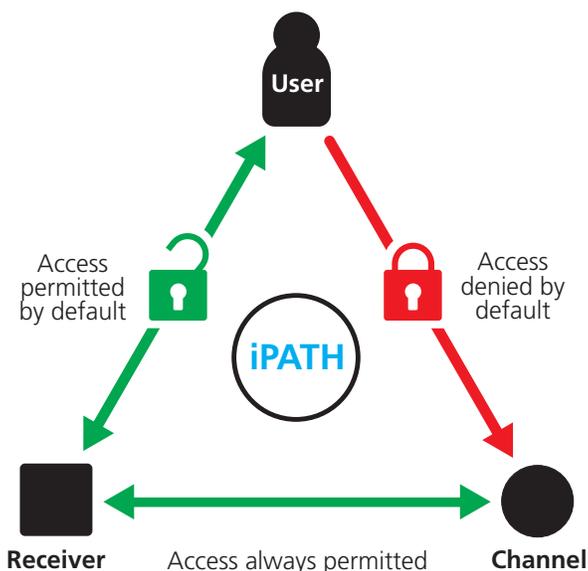
Figure 2-3. The diagram shows the three way relationship,
controlled by iPATH Agility Controller, between users, receivers and channels.

To successfully gain access to a channel:

- The user requires permission to use the receiver,

- The receiver requires permission to connect with the channel,

    AND

- The user must have permission to access the channel.

In most cases, the need for three access permissions per connection is unnecessary and raises administration overheads. Hence, by default, iPATH Agility Controller grants open access for the user to the receiver and the receiver to the channel while restricting the final, most crucial piece of the puzzle. For those who require it, the lock upon the user to receiver stage can be applied individually or globally.

2.3.5 Active Directory

To streamline administration even further, iPATH Agility Controller supports Active Directory. By synchronizing with an LDAP/Active Directory server, details of users (including their usernames and group memberships) can be securely synchronized from existing databases in order to both minimize the initial configuration as well as streamline ongoing updates.

2.3.6 iPATH Agility Controller Interface

iPATH Agility Controller appears in two main ways, depending on whether you are an administrator or a regular user.

- For administrators, full access to the iPATH Agility Controller Suite is granted. This comprehensive application shows eight main tabbed areas: Dashboard, Channels, Receivers, Transmitters, Servers, Users, Presets and Statistics, each of which contains numerous related pages of settings and options. The Dashboard provides a central location from which the administrator can view overall operation, make various changes, database backups and also upgrade the firmware of any linked Agility unit.

- For regular users, an efficient page layout provides a list of all channels for which you have permission to visit. Against each selectable channel name and description, a series of icons provide clear feedback about current availability.

2.3.7 Permissions

Permissions exist between Users, Receivers, and Channels.

By default, all users are granted permission to access ALL receivers.

By default, all receivers have permission to connect to ALL channels.

As shown in the introductory diagram, the missing part is the permission for a user to access each channel.

Permissions between a user and a receiver can be applied in any of the following ways:

- User –> Receiver
- User –> User Group –> Receiver
- User –> User Group –> Receiver Group –> Receiver
- User –> Receiver Group –> Receiver

Thus, a very indirect way of granting permissions could be:

- User1 is in UserGroup1,
- UserGroup1 has access to ReceiverGroup1,
- ReceiverGroup1 contains Channel1,
- Therefore, User1 has access to Channel1 indirectly.

2.4 iPATH Agility Controller Unit Features

The iPATH Agility Controller unit is housed within a durable, metallic enclosure with most connectors situated at the rear panel.

The smart front face features two indicators, a power switch and two USB ports, as shown in Figure 2-4:

Green indicator: Power

Red indicator: Drive activity
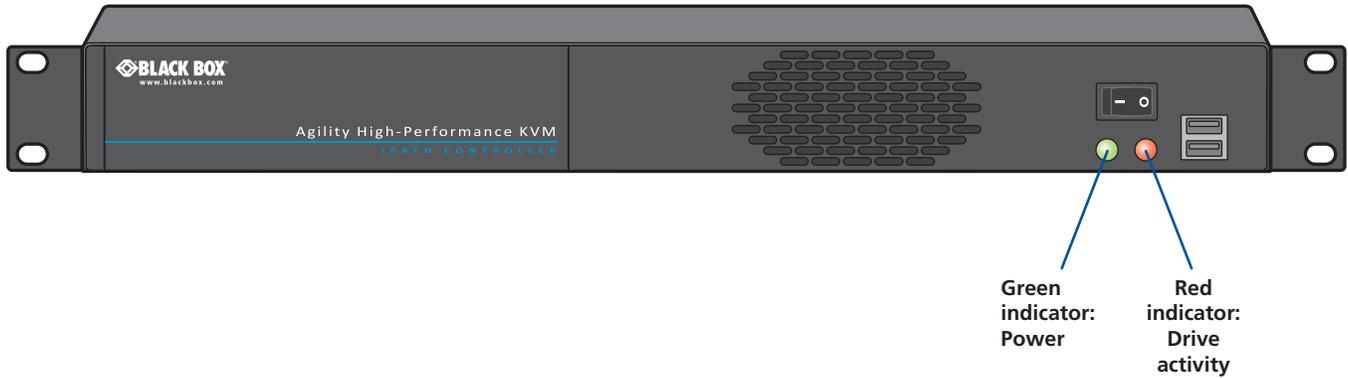
Figure 2-4. iPATH Agility Controller unit - front panel.

Figure 2-5 shows the connectors located on the rear panel of the local transmitter unit:

Power input

Video output port

Internal network port

External network port
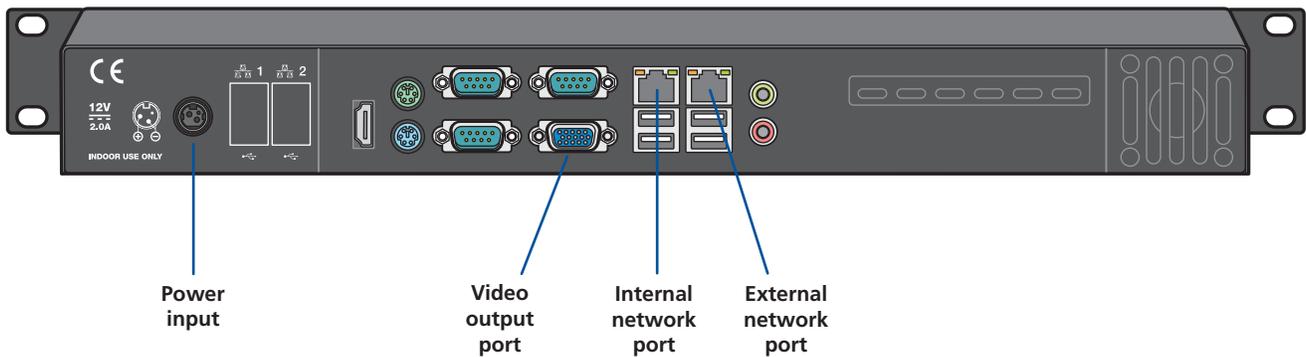
Figure 2-5. iPATH Agility Controller unit - rear panel. During normal use, only the network and power connections are used.

877-877-2269 l blackbox.com

2.5 What's Included

Your package should include the following items. If anything is missing or damaged, contact Black Box at 877-877-2269 or info@blackbox.com.

2.5.1 iPATH Agility Controller Package (ACR1000A-CTL-24 to -288 and -ULT)

- iPATH Agility Controller unit,

- Power adapter and power cord,

- (2) Rack mount brackets plus screws,

- Safety leaflet.

2.6 Additional Items You May Need

- Network link cable(s).

3. Installation

3.1 Installation Requirements

- The minimum permissible firmware versions for Agility units linked with the iPATH Agility Controller depend upon the firmware version that is running on the iPATH Agility Controller itself:

  - iPATH Agility Controller: v4.0   Attached Agility endpoints: v3.5 (minimum)

  - iPATH Agility Controller: v4.1*   Attached Agility endpoints: v4.1 (minimum)

  - iPATH Agility Controller: v4.2*   Attached Agility endpoints: v4.2 (minimum)

  * iPATH Agility Controllers with firmware version 4.1 or above no longer support the original Agility ACR1000A.

- On the network switch(es) that have iPATH Agility Controller(s) attached, ensure that the *portfast* option is enabled on each port to which an iPATH Agility Controller unit is connected. Where portfast is not enabled, if a second iPATH Agility Controller is added for redundancy, this could result in a mis-configured back up server.

- If an existing iPATH Agility Controller must be replaced, follow the important advice given within **Appendix C (Swapping out an iPATH Agility Controller)**.

- When configuring the installation for multicasting (and to improve overall performance), the network switch(es) being used must support a minimum of IGMP v2 snooping. For faster performance use switches that support IGMP v3.

- In order to display video resolutions that use a horizontal video resolution of 2048 pixels, the network switch must have support for Jumbo packets.

- Please also see **Appendix A - Tips for success when networking Agility units**.

- This unit should always be installed in suitable a 19" rack space, it is not suitable for standalone desktop use.

3.2 Connections

The iPATH Agility Controller unit is supplied fully pre-loaded and permits no local user interaction. All configuration takes place remotely via the network connections and as a result only two connections are required: Network and power.

Note: The iPATH Agility Controller is supplied with the front panel USB connections blanked off. There is no need to connect a keyboard or mouse to the unit as configuration takes place across the network connection.

3.2.1 Network Connections

The iPATH Agility Controller has two network connections on the rear panel: port **1** on the left and port **2** on the right. These allow the unit to be connected to internal and external network connections (respectively) as required. The external network connection allows admin users located away from the internal network to be able to login. Network port 2 supports DHCP, however, port 1 does not and needs to be configured manually.

1 Run a category 5, 5e or 6 link cable from the appropriate hub or router to the iPATH Agility Controller unit.

2 Connect the plug of the link cable to the left IP port (1) on the rear panel of the iPATH Agility Controller unit, as shown in Figure 3-1:
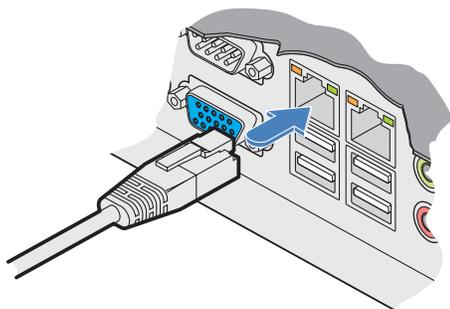
Figure 3-1. Connecting Category 5, 5e or 6 cable from LAN / network switch.

877-877-2269 l blackbox.com

3.2.2 Power Supply Connection

Important: Please read and adhere to the electrical safety information given within the Safety information section of this guide. In particular, do not use an unearthed power socket or extension cable.

1 Attach the output connector of the power supply (country specific power supplies are available) to the power input socket on the left side of the rear panel, as shown in Figure 3-2:
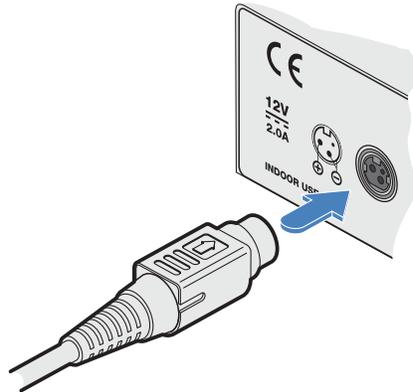
Figure 3-2. Connecting the power adapter plug to the power input socket.

2 Connect the main body of the power supply to a nearby earthed power outlet, as shown in Figure 3-3:
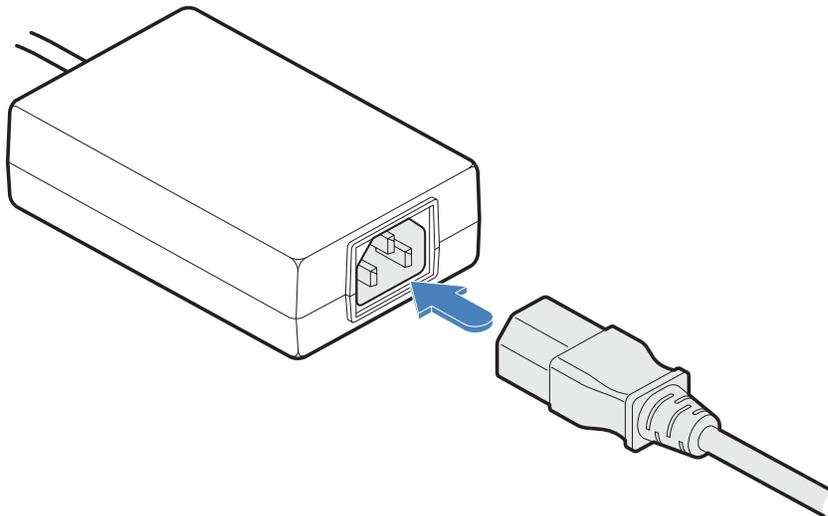
Figure 3-3. Connecting the power adapter plug to the power input socket.

To switch on the iPATH Agility Controller unit, click the power switch on the front panel. Allow 3 minutes for the booting process to complete.

3.3 Mounting the iPATH Agility Controller

The iPATH unit is designed to be easy to mount within a standard 19" rack, it is NOT suitable for free standing use on the desktop. The server chassis requires just a 1U space within the rack.

3.3.1.1 To mount the iPATH Agility Controller within a rack mount

1 Slide the iPATH Agility Controller into the vacant 1U space within the rack mount.

2 Secure each bracket to the rack using two screws per side as shown Figure 3-4:
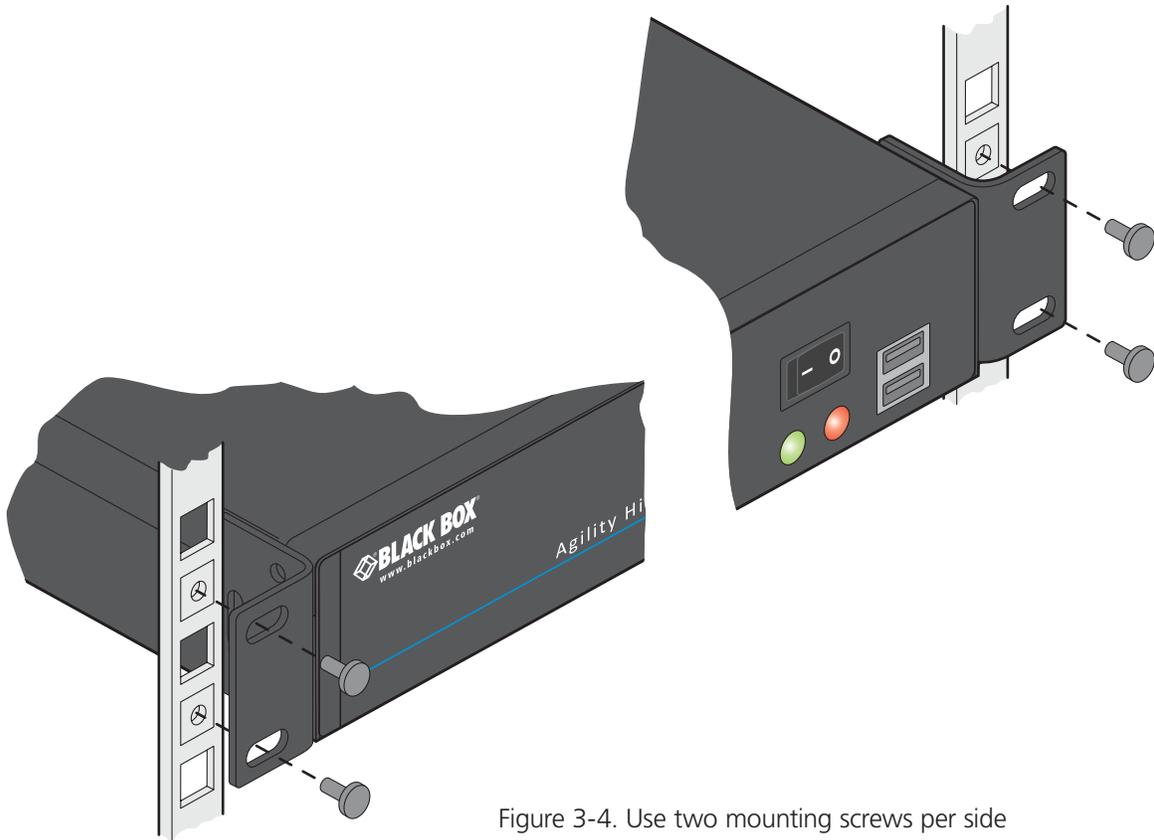
Figure 3-4. Use two mounting screws per side

4. Configuration

This section covers configuration of the iPATH Agility Controller Suite for administrators. For details about the regular user interface, please see the Operation section.

4.1 Supported Browsers

The iPATH Agility Controller admin interface requires an A-grade browser with Javascript enabled.

The list of appropriate browsers is as follows (*Note: For best results always use the latest versions of the supported browsers.*):

- Google Chrome
- Firefox
- Internet Explorer
- Safari

4.2 Login For Admin Users

1 Ensure that the iPATH Agility Controller is powered on (allow 3 minutes before accessing).

2 Using a computer located anywhere within the local network, open a web browser (see Supported browsers list opposite) and enter the default IP address for the iPATH Agility Controller: **169.254.1.3**

   The Login page will be displayed, as shown in Figure 4-1:
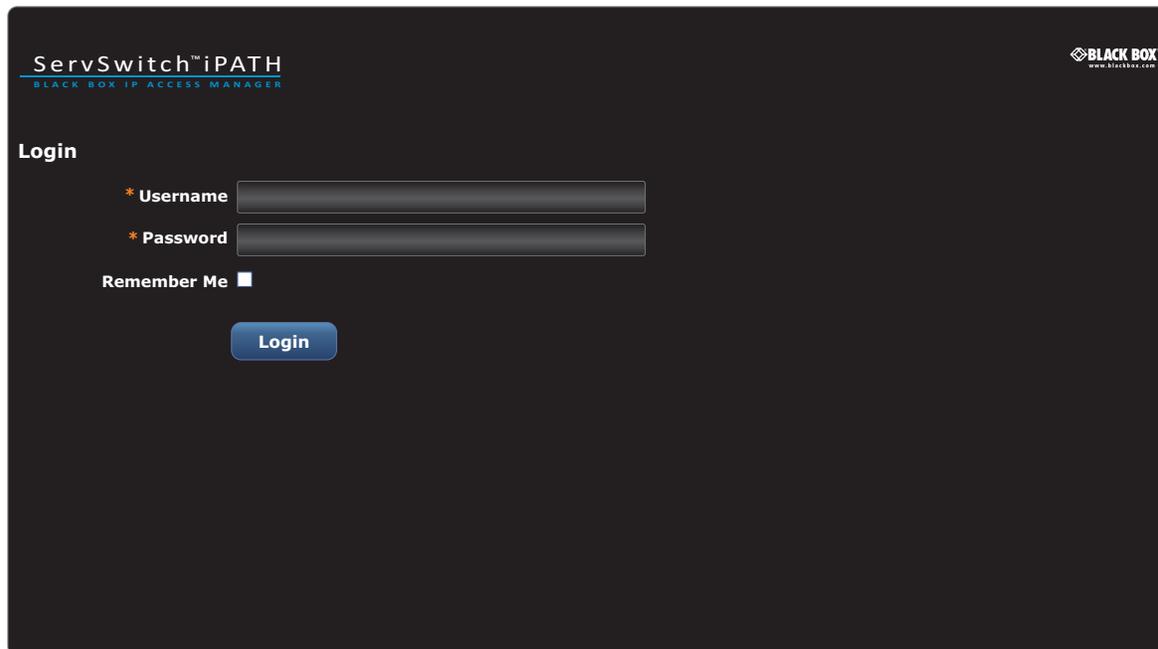
Figure 4-1. Login page.

3 Enter your Username and Password and click the Login button.

   The default username is **admin** and the default password is **password**.

   We strongly recommend that you change the default admin password as one of your first actions: Go to Dashboard>Users. Click on the furthest right icon in the admin row (configure users) and change the password for the admin user.

   If you check the **Remember Me** box, a cookie will be stored on the computer, allowing you to access the admin section without having to log in each time. The cookie will survive up to the *iPATH Admin Timeout* period. If you do not check the Remember Me box, you will remain logged in only for the duration of your browser session.

   Please see the important notes shown on the next page.   *continued*

4.3 Important first configuration steps

There are several important configuration steps that must be carried out when starting a new iPATH Agility Controller for the first time.

4.3.1 To determine the iPATH Agility Controller's rôle and main IP address

1 Switch on and log in to the iPATH Agility Controller; you will be presented with the Servers page.

2 Within the Server page, choose the Rôle of this new iPATH Agility Controller:

   - **Solo** - This will be the only iPATH Agility Controller on the network (with no redundancy and failover), or

   - **Primary** - This server will be used as part of a redundant cluster of iPATH Agility Controllers, where it will be the main server used to manage the Agility units.

3 Click the Save button. You will next be presented with the Dashboard > Settings > Network page.

4 Within the *Ethernet Port 1* section half way down the page, change the default *iPATH IP Address* (and *Netmask*) options to settings that suit your network configuration and which will be used henceforth for this server.

   Note: The iPATH IP Address and Netmask can only be set up once and you will NOT be able to perform any other actions, or navigate to any other pages, within the iPATH admin interface until you have set and saved it.

   IMPORTANT: Once set, the Ethernet Port 1 iPATH IP Address and Netmask settings must NOT be changed during operation of the system. Changing these will invalidate the system's security and require intervention from Black Box technical support staff to restore to a working state.

5 You can now either:

   - Continue with other settings on the same page (See *To choose how IP addresses are applied to Agility units* on the next page), or

   - Click the Save button. After a short delay the web browser will automatically redirect itself to the new IP address so that you can continue administering the iPATH Agility Controller.

   Note: Ensure that your computer can view the new IP address, otherwise the iPATH Agility Controller will appear to be offline. Depending on your network configuration and that of the computer, you may need to change the computer's configuration to be able to see iPATH Agility Controller's new network address.

4.3.2 To choose how IP addresses are applied to Agility devices

1 Login again to the iPATH Agility Controller and choose the Dashboard > Settings > Network page.

2 Depending upon the level of your purchased license, the *Subnet Operation* option may, or may not, be presented at the top of the page. If the *Subnet Operation* option is present, you have the following choices:

- **Off** - iPATH can administer a single subnet and will use its own DHCP (Dynamic Host Configuration Protocol) server to automatically assign IP addresses to new Agility devices, drawing upon a pool of spare addresses defined by you.

- **On** - iPATH can administer devices across multiple subnets, but will rely upon an external DHCP server to assign valid IP addresses to new Agility devices.

    Note: If the Subnet Operation option is not present, the iPATH Agility Controller will operate as per the Off setting described above. For details about upgrading your license, see Appendix D.

3 If you chose the *Off* setting (or if *Subnet Operation* is not part of your license), you now need to define the boundaries of the IP address pool that will be used by the internal DHCP server. Enter valid start and end addresses to the *IP Pool Lower Limit* and *IP Pool Upper Limit* options.

    Note: If you chose the On setting, you will need to perform a similar operation within the external DHCP server.

    For further details about other options within this page, see Dashboard > Settings > Network.

4 When all options have been set, click the *Save* button.

IMPORTANT

If an existing iPATH Agility Controller must be replaced, follow the important advice given within **Appendix C (Swapping out an iPATH Agility Controller)**.

4.3.3 When adding Agility units

When new Agility transmitters and receivers are added to a network, they are designed to automatically announce themselves* to the iPATH Agility Controller. Once the iPATH Agility Controller receives their announcement(s), the Agility units will be added to the administrator's view of the Dashboard. From here you can then begin to configure each new Agility unit.

Agility units can be configured either from their own browser-based configuration utility or via the iPATH Agility Controller. Once an Agility unit has been configured in one way, it cannot be reconfigured using the other method without undergoing a factory reset. This policy is in place to help prevent accidental overwriting of configurations. It also means that once an Agility unit has been locally configured, it will not announce itself to the iPATH Agility Controller upon being added to a network. Please see right for details about resetting an Agility unit.

When new Agility devices announce themselves, depending upon how it was initially configured (see *Important first configuration steps*), the iPATH Agility Controller will either assign IP addresses to new Agility units automatically, or will rely upon an external DHCP server to do the same. Either way, providing each Agility device is not already configured and announces itself to the iPATH Agility Controller (see below for potential issues that can prevent this), they will be automatically provided with a suitable IP address so that they may operate within the network. Once Agility units have been added, you can use the iPATH Agility Controller Dashboard to select and further configure any or all of them.

4.3.4 If a Agility unit is not located

There are several reasons why an Agility unit might not be located by iPATH:

- The Agility unit has been locally configured or is otherwise not using its factory default setting. Try performing a factory reset on a Agility that is not being located.

- The Agility unit is not located in the same Ethernet segment as the iPATH Agility Controller. Double check connections and move units where necessary, so that all reside within the same Ethernet segment.

- There is a potential cabling problem between the Agility and iPATH units. Check and where necessary, replace faulty cables.

4.3.5 Agility manual factory reset

Where a previously configured Agility unit is being added to a network for control by an iPATH Agility Controller, you can use this method to reset the unit to its default configuration.

4.3.5.1 To perform a manual factory reset

1 Remove power from the Agility unit.

2 Use a narrow implement (e.g. a straightened-out paper clip) to press-and-hold the recessed reset button on the front panel. With the reset button still pressed, re-apply power to the unit and then release the reset button.

Agility

Agility Dual or Agility Dual VNC

After roughly eight seconds, when the factory reset has completed, five of the front panel indicators will flash for a period of three seconds to indicate a successful reset operation.

4.4 The Dashboard Tab

The Dashboard is your main point of contact for checking and changing the general status of all iPATH Agility Controller operations.

Click the DASHBOARD tab to view its initial home page.

The various other Dashboard pages (e.g. Settings, Backups, Updates, etc.) are selectable within the blue section located just below the tabs.

4.4.1 Dashboard > Home

- **Shutdown button** - Allows the admin user to shut down the iPATH Agility Controller. The OSD will no longer work on Receivers. The iPATH Agility Controller will need to be manually started again when next required.

- **Restart** - The admin user can reboot the iPATH Agility Controller. The OSD and admin section will be unavailable while the server is rebooting. This currently takes about 75 seconds.

Within the Home page*, the different sections provide a variety of information:

- **Warning messages** - Live alerts are displayed concerning any devices that are offline, rebooting, recently added or unconfigured.

- **Latest Active Connections** - shows the five most recent active sessions, detailing for each: When the session started; which user/receiver/channel is involved; the connection type (icons show audio, video, serial, USB, exclusive) and IP addresses in use. The red unplug icon on the far right allows the admin user to disconnect a connection.

- **Event Log** - shows all actions performed by the admin or end-users within the iPATH Agility Controller system. See also the Event Log page.

- **Latest Channels Created** - shows the last five channels created within the iPATH Agility Controller system. A channel is created by default when a new transmitter is added and configured. The edit icon next to a channel allows the admin user to configure the channel.

- **Latest OSD Logins** - shows the last five users who logged in (either to the iPATH Agility Controller admin or at an Agility Receiver).

- **Latest User Registrations** - shows the last five users added to the iPATH Agility Controller system, with a link to edit the user's details/permissions.

- **Latest Channel Changes** - shows the last five users who changed a channel, either while using the on-screen display (OSD) at an Agility Receiver, or via the iPATH Agility Controller admin control panel.

- **Latest Receivers Added** - shows the last five receivers to be added and configured within the iPATH Agility Controller network. Click 🖊 to configure a receiver; click 🌿 to connect to a channel; or click 🖇 to disconnect an existing connection.

- **Latest Transmitters Added** - shows the last five transmitters to be added and configured within the iPATH Agility Controller network. Click 🖊 to configure a transmitter.

* The Home page is auto-refreshed every ten seconds to ensure that the latest information is always available.

4.4.2 Dashboard > Settings

Click the Settings option below the Dashboard tab.

The Settings section contains global configuration options for the iPATH Agility Controller system and is divided into eight pages, each accessible by clicking the relevant button located below the blue options bar:

General • Transmitters • Receivers • Servers • Network • Time • Mail • Active Directory

For configuration options that affect individual receivers, users channels, etc., see the sections dealing with those tabs.

4.4.2.1 Dashboard > Settings > General
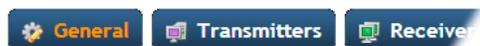
Receiver OSD Timeout
Determines the time period of inactivity within the OSD after which a standard user will be automatically logged out.

iPATH Administrator Timeout
Determines the time period of inactivity within the iPATH Agility Controller config pages after which an admin user will be automatically logged out.

Anonymous User
Determines which user is shown in the log when a receiver is set to 'No login required'.

Hide Dormant Devices
If enabled, devices that have been offline for more than 24 hours will be hidden.

Grant All Users Private Access
Determines whether a user can connect to a channel privately and thus prevent any other users from also connecting to that channel. If not set, users can only connect in View-only mode or Shared mode. Settings that are applied specifically to a user will override settings applied to user groups they're in, which in turn override this global setting.

Note: If a user has Private Access mode granted or NOT granted at user level, then it doesn't matter what settings there are above (usergroups or global).

- If a user is set to inherit "Allow Private?" mode from their user groups, if any one of their user groups has "Allow Private?" mode granted, then the user will have it granted, even if the rest of the user's usergroups have Private mode not granted.

- If a user is set to inherit "Allow Private?" mode from their user groups, and one of the user groups is set to inherit from the global setting - if that global setting is "Allow Private?" mode, then effectively the user group is "Allow Private?" mode, so the user will be allowed Private mode.

Grant All Users Remote OSD Access
If enabled, allows receivers to be switched remotely from another receiver's OSD menu.

Allowed Connection Modes
Determines the global setting that will be applied to all new channels concerning connection modes. The setting made here is only applied as a default and can be overridden at the channel level, where necessary. Options are:

• Video-Only: Allows users only to view the video output, the USB channel is denied.

• Shared:* Allows users to control a system in conjunction with other users.

• Exclusive: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.

• Private: Allows a user to gain private access to a system, while locking out all others.

Note: By default, all new channels are set to inherit this global value. So it's easy to change all channel connection modes simply by changing the global setting. If a channel has its own setting, the global setting has no effect on that channel.

* If USB is disabled, Shared mode will not be available as an option.

Rows per page
The number of rows to display in all paginated tables in the admin section.

Locale
Determines the language shown on the OSD menus of the receivers. Note the admin configuration web pages remain in English.

Debug Level
This allows information to be collected for diagnostic purposes. Do not use the full level unless advised by a technical support engineer.

API Login required
If enabled, the anonymous use of the iPATH Agility Controller API will be disallowed.

Anonymous user
Determines the user permissions to be used when the API is accessed without logging in.

Supported devices
Indicates the limits of the current license.

Upgrade Licence (see Appendix D for details)
Displays information about the number of devices that can be connected to the iPATH Agility Controller.

Licensed Features
Displays the level of operation permitted under the current license. Click view/change to see more detail and gain a unique identifier that can be declared to Black Box when upgrading a license.

4.4.2.2 Dashboard > Settings > Transmitters

This page applies a standard global configuration to all transmitters.

Magic Eye
Determines whether the Magic Eye feature should be enabled on Agility (excluding Agility Revision 1) transmitters. Magic Eye works to overcome the issues with increased bandwidth usage caused by 'dithering' techniques used on some computers, such as Apple Macs. See the Agility Dual user guide for more details.

DDC
Determines whether video configuration details should be harvested from connected display screens or a static fixed EDID report should be used. Care must be taken when selecting a Dual Link Video resolution as only Agility Dual units support a Dual Link Video resolutions. In the case of a Dual Link EDID being set in the Global settings, no EDID will be set on Video port 2 of the Agility Dual transmitters.

EDID optimisation
When this option is ticked, the Transmitters will compare the native resolution settings of their monitors when switching. If the monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. This speeds up switching as the graphics card does not have to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver has a monitor with a different native resolution, then the EDID will be updated to allow for a change in video mode.

Hot Plug Detect Control
Determines whether to enable hot plug detection for monitors. By default this is enabled.

Hot Plug Detect Signal Period
By default this is set at 100ms, which is sufficient for most graphics cards. Occasionally it may be necessary to adjust this. A technical support engineer will advise if necessary.

Background Refresh
The number of frames between sending an entire frame of video data. Setting this to a longer period or disabling this will reduce the bandwidth required.

Compression Level
The newer AFZ+ codec compliments the existing AFZ codec by providing greater compression for increased speed where pixel perfect results are not the primary focus. The transmitter video configuration page allows you to choose the required compression mode. Choices are:

• 'Pixel perfect' - only uses pixel perfect AFZ,

• 'Adaptive' - guarantees frame rate, builds to pixel perfect,

• 'Smoothest video' - forces the maximum compression, or

• 'Advanced' - allows you to choose the mode:

  • 'AFZ only (pixel perfect),

  • 'AFZ+ Minimum compression',

  • 'AFZ+ Middle compression', or

  • 'AFZ+ Maximum compression'.

USB Speed
Select Low/full speed or High speed USB operation.

USB Hub Size

Select either a 13 or 7 port USB hub. This determines the number of USB devices that can be connected to a single Transmitter.

Note: It is not possible to reserve USB ports on the transmitter when used with iPATH Agility Controller.

Enable Dummy Boot Keyboard

It is often necessary to have a keyboard reported at start up. This setting means that a "Virtual Keyboard" is always reported to the USB host. It may be necessary to disable this for use with some KVM switches.

Reserved USB ports

This setting lets you set aside a specific number of USB ports (up to 8) on the transmitter that can be made available for certain USB devices which require a quirk setting under advanced usb features, connected to a receiver.

Note: This setting can only be applied globally; it is not found with individual transmitter configurations because all receivers need to know how many USB ports are available for the advanced USB features.

Serial port options

These allow you to match the serial configuration being used by the attached PC host.

4.4.2.3 Dashboard > Settings > Receivers

This page applies a standard global configuration to all receivers.

Hotkey settings
The first few rows determine the Hotkeys that can be used to invoke certain functions. It is possible to select mouse keys to perform these functions, though it is not possible to use both mouse switching and a hot key combination. It is also not possible to mix left and right function keys. Left Ctrl and Left ALT are the default settings.

Login required
Determines whether it is necessary to log into the receiver.

Enable Receiver OSD Alerts
Determine the required setting for pop up OSD alerts: No or Yes.

Video Compatibility Check
This reads the EDID from the attached monitor and determines whether the monitor is capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out because a dual link resolution has been selected to display on a single link monitor.

Force 60Hz
If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (below) cannot be altered when this option is enabled.

Video switching
Provides two options for video switching:

• Fast Switching (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.

• Match Frame Rate - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@60Hz and 1920x1080@50Hz then this setting will change the frame rate from 60Hz to 50 Hz every time that you switch.

Receiver Keyboard Country Code
Select the country code of the keyboard connected to the receiver.

Audio Input Type
Select the required audio input type.

USB Settings

HID only

If enabled, allows only HID (mice and keyboards) devices to be connected to the receivers.

Disable Isochronous Endpoint Alerts

When an isochronous USB device is connected to the receiver there will no longer be a warning message. Agility units do not support isochronous devices.

Enable Isochronous Endpoint Attach

Some USB devices combine many USB devices behind a USB hub. e.g a keyboard with audio support. By enabling this option, devices will be allowed to connect to Agility receivers, however, the isochronous part (e.g. the audio component) of the devices will not work.

Advanced Port

This section allows you to determine USB port behaviour for use with certain USB devices.

The default is no reserved ports, Merging enabled and no feature code (or Quirk) set. It is recommended that these are left at the default settings and are only changed under advice from a tech support engineer.

For each of the four USB ports on the receiver, certain rules can be applied depending upon the USB device connected.

If you have reserved USB ports on the transmitter, you can select which USB port to use for a particular device.

You can turn off USB merging for a particular port. This will slow down switching as the USB device will be enumerated every time that you switch.

You can also enter an advanced feature if it is necessary for your USB device. The drop down lists the feature codes for some known USB devices. Otherwise please contact your tech support engineer for advice.

4.4.2.4 Dashboard > Settings > Servers

This page is used to configure redundant operation for the iPATH Agility Controllers.

It is now possible to place two iPATH Agility Controllers on the same subnet. One iPATH Agility Controller is the Primary (or Master) the other is the secondary (or Slave). If the Primary server fails for any particular reason then the Secondary will take over until the Primary is repaired. This functionality is only possible if the licenses of the both iPATH Agility Controller units match. Both iPATH Agility Controller units need to be able to control the same number of endpoints.

Primary Timeout
The time (in seconds) for the Primary server to be unavailable before the secondary takes over.

Quiescent Timeout
The time after which an inactive (Quiescent) server is assumed to have disappeared.

Backup Check Interval
The interval between the Primary server querying its backups to determine if they are all on-line.

Backup Timeout
The period of time that a backup server can be off line or uncontactable before it is treated as a failed server.

Require Authentication
If set to 'Yes', then a new, unconfigured iPATH Agility Controller will be unable to join the cluster automatically; it's behavior will be to report itself as unconfigured and quiescent, and request a password. Entering the cluster password will then allow it to join the cluster as a Backup.

Cluster Password
This is the password that is used for iPATH-to iPATH https queries, if the Require Authentication option is enabled.

4.4.2.5 Dashboard > Settings > Network

This page applies global network parameters to the iPATH Agility Controller network.

Require SSL for Web
If set to yes, a certificate needs to be downloaded and all connections will then take place using HTTPS:// connections rather than the default HTTP:// connection types.

IP Pool Lower/Upper Limits (not shown in multi-subnet mode)
When the iPATH Agility Controller is used in single subnet mode, these two fields are used to define the range (pool) of IP addresses that the iPATH Agility Controller can automatically assign to new Agility endpoint devices. The iPATH Agility Controller contains its own DHCP server with which it applies the available IP addresses to Agility endpoint devices.

When used in multi-subnet mode, the internal DHCP server with the iPATH Agility Controller is disabled and instead the iPATH Agility Controller will rely upon an external DHCP server to provide valid IP address details.

Multicast IP Base
The start address for the multicast IP addresses to be used. Multicast IP addresses are in the range 237.1.1.1 to 239.255.255.255. This setting lets you adjust this range of IP Multicast addresses. It is important to allow sufficient addresses for your system. For instance, if the multicast IP address base was set to 239.255.255.252 there would only be 4 multicast addresses available.

Always Multicast
Determines whether multicast addressing is always used for video and audio streams. This should be used for most installations as it provides the most efficient way to deliver video and audio to multiple destinations.

Separate Device Networks
When this option is set to 'Yes', the Agility devices within the network will be instructed to promote a further level of network resilience by treating their copper and fiber/teaming connections as independent links via separate switches (in conjunction with dual independent cabling schemes) see the diagram on next page. If one connection route is compromised, the other will continue unaffected. During normal operation, when both connection routes are operating, transfer speeds are boosted by the copper and fiber links working in parallel.

The two Ethernet ports of the iPATH Agility Controller can be connected to the two separate network switches to ensure that iPATH control remains in place if one network switch should become unavailable.

Route of Last Resort
This option is appropriate when the iPATH Agility Controller is used in multi-subnet mode. In such cases it is possible that the iPATH Agility Controller is not directly connected to the same sub-network as some or all of the Agility endpoints. Therefore, it will be necessary for the Agility unit(s) to communicate back to the iPATH Agility Controller via a gateway device. This option is used to indicate which interface has the gateway configured.

Device Network Port
This option determines the most appropriate mode of redundancy between multiple iPATH Agility Controllers in a cluster. The default setting is 'Port 1' and this is correct for a typical configuration in which the Agility endpoints and iPATH Agility Controller(s) are all located on one subnet. Alternatively, where iPATH Agility Controllers are linked to two separate subnets, both of which can provide a route from the endpoints, then choose the 'Both' setting.

Gateway IP Address
Defines the IP address of an optional gateway device.

Ethernet Port 1

The primary iPATH Agility Controller Ethernet port can only be configured using a static IP address. Use the three option provided to configure the IP address, netmask and DNS server address.

Ethernet Port 2

The secondary iPATH Agility Controller Ethernet port can be configured to either: gain its details via a DHCP server; use a Static IP address, netmask and DNS server address, or alternatively be set to Bonded operation, whereupon three further Bonding Mode options are displayed:

- **Active-Backup** - This can be used when both of the iPATH Agility Controller's network connections are linked to the same network switch. This option provides a fail-over to cater for the possibility of hardware failure or connectivity failure between the iPATH Agility Controller and the switch.

  In this mode, one of the iPATH Agility Controller's network ports will be active while the other remains dormant. If the active port experiences a failure, such as a loss of connection, its configuration is automatically transferred to the secondary port. Once the original primary port resumes connectivity, this will become the backup and be placed into a dormant mode.

- **Broadcast** - This option would be used when the twin ports of the iPATH Agility Controller and all attached Agility devices are split between duplicate networks:
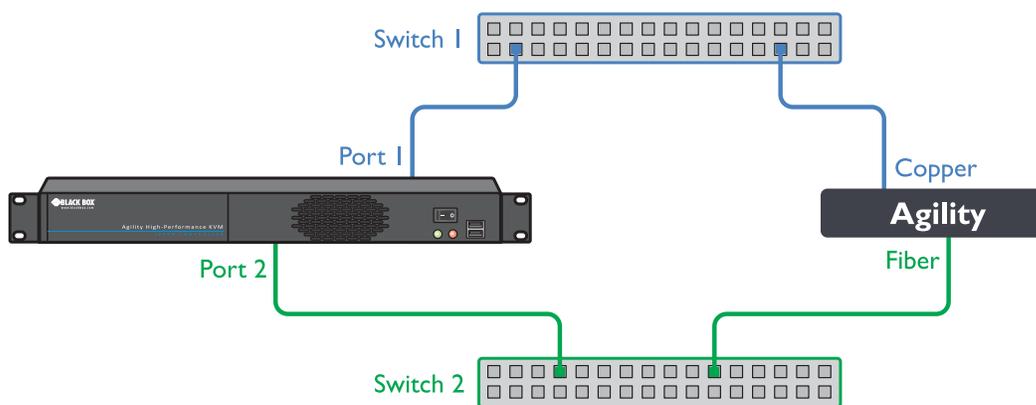
The 'Separate Device Networks' option mentioned earlier would be enabled on the iPATH Agility Controller and the respective network connections on the endpoints are connected accordingly (e.g. copper to copper on only switch 1 and SFP to SFP only on switch 2).

In Broadcast mode, both of the iPATH Agility Controller network connections mirror each other, i.e. duplicate network traffic is sent out on both connections. It is assumed that the connected devices will only listen to the network traffic intended for themselves and drop/ignore all other traffic intended for other devices. This mode is robust but inefficient because half of the packets are discarded.

- **802.3ad** - This mode uses a similar topology to Active-Backup, (i.e. both network ports connected to the same switch) but has two important differences: Both of the iPATH Agility Controller network ports are used simultaneously, and the network switch must support LACP (Link Aggregation Control Protocol).

  The iPATH Agility Controller will 'merge' (aggregate) the two connections and treat them as one. The only exception to this would be on 'multi-Subnet racks' where it would be possible to have each network connection on different switches.

  This mode provides the benefit of increased bandwidth availability between the iPATH Agility Controller and the network, but also provides a layer of redundancy. If one of the network connections is lost, the remaining connection would take over until the link is restored.

  The network traffic is not split on a packet by packet basis between the connections; it operates on a connection basis. When a connection is established between the iPATH Agility Controller and one of the Agility endpoints, this would travel via one port. When a second connection to another endpoint is established, this could use the same port or it may use the other. There is no order to which network port is used for any connection.

Note: When changing between bonded and any other mode, a warning message will be displayed and, when the Save button is clicked, will cause the iPATH Agility Controller to be rebooted.

Syslog Enabled
Determines whether Syslog should be used to record log data to an external Syslog server.

Syslog IP Address
The address of the external syslog server.

SNMP
This option allows the iPATH Agility Controller to connect to an external SNMP server. If SNMP is enabled, there are three connection modes:

- Authentication + privacy

- Authentication only

- No authentication

There are two authentication types SHA or MD5 and two Privacy types AES or DES.

4.4.2.6 Dashboard > Settings > Time

This page deals with all time related settings for the installation and allows up to three external NTP servers to be defined.

NTP Enabled
Determines whether one or more external Network Time Protocol servers should be used to provide timing for the installation.

Server 1 Address
Enter the IP address of the NTP server.

NTP Key Number/NTP Key
If you wish to use Symmetric key authentication for the server, enter an appropriate NTP key number and key.

If you need to add more NTP servers, click the Set option next to the NTP Server 2 or 3 entries.

Time Zone Area and Time Zone Location
Use these entries to pinpoint the current location of the installation.

4.4.2.7 Dashboard > Settings > Mail

This page sets up the email functionality of the iPATH Agility Controller if required. An external Email server is required to sit on the network if this functionality is to be used.

Mail Enabled?
Determines whether the mail features of iPATH Agility Controller should be invoked.

SMTP Domain name/IP
Enter the name or IP address of the external SMTP server that will be used to process all outgoing mail.

SMTP Port
Enter the appropriate port on the SMTP server.

Username, Password
Enter the appropriate username and password for access to the SMTP server.

Email Address for Alerts
Enter the email address that will be used to send alert messages.

4.4.2.8 Dashboard > Settings > Active Directory

This page sets up the active directory server, if there is one on your network, and to use active directory to maintain the user database.

AD Enabled?
Determines whether Active Directory features will be used.

Account Suffix
Enter the account suffix for your domain.

Base DN
Specify the base Distinguished Name for the top level of the directory service database that you wish to access.

Domain Controller
Enter the IP address or name of the server that holds the required directory service.

Username, Password
Enter the username and password for the domain account.

Sync Schedule
Choose the most appropriate synchronization schedule, from hourly intervals to daily or weekly.

4.4.3 Dashboard > Backup

You can schedule backup copies of the iPATH Agility Controller database (containing all devices, users, channels and logs) to be made on a recurring basis and you can also perform backups on demand, as required.

IMPORTANT: You are strongly recommended to arrange regular scheduled backups of your iPATH Agility Controller database. Black Box cannot be held responsible for any loss of data, however caused.

Backup Options

Download to your computer: If this option is checked, when you click the "Backup Now" button, the backup file will be saved to the server and then will be presented as a download in your browser, so that you may save a local copy of the backup file.

Email backup: If this option is checked, a copy of the backup file will be sent to the email address specified in the "Email Backup To" field. The backup file will be emailed either when you click "Backup Now" and/or according to the option selected in the Schedule section.

Note: Use of the Email backup option requires a valid email address to be stored within the Dashboard>Settings page.

Note: Emailed backups are encrypted, and these backup files are automatically decrypted by the iPATH Agility Controller when they are used.

Schedule: Determines how often a backup should be created. There are set periods for the various options:

- Hourly backups are executed on the hour (or quarter past).

- Daily backups are executed at 2am (or quarter past).

- Weekly backups are executed every Sunday at 3am (or quarter past).

Restore from Server

All backups (whether initiated manually or by schedule) are saved on the server together with a time-stamp of when the backup was run. If required, you can select a previous backup and restore its contents. Alternatively, you can download the backup file to another location.

IMPORTANT: It is advisable to make a backup of the current state of the iPATH Agility Controller system before restoring a previous backup. Restoring the contents of a backup file will overwrite ALL data in the iPATH Agility Controller system, with the data within the backup file. This includes configured devices, channels, users, connection logs and action logs.

Restore from File

Use this option to upload a backup file that you have previously downloaded or received by email. This will overwrite the contents of the current iPATH Agility Controller system therefore it is advisable to make a backup of the current state of the iPATH Agility Controller system before restoring a previous backup.

Archive Log to CSV File

You can archive connection or log data to a CSV file and, at the same time, remove old log data from the database.

Click "Archive" to save a CSV file to the server.

Download CSV Archive

You can download any CSV archive that was created in the archive step (described above) by selecting from the archives saved on the server.

The CSV archive can be opened in Microsoft Excel (or similar) to perform detailed analysis of actions and connections within the iPATH Agility Controller system.

4.4.4 Dashboard > Updates

Upgrade iPATH Software

This option allows you to upgrade (or downgrade, if required) the iPATH Agility Controller firmware while preserving all configuration data. Firmware files are encrypted and digitally-signed for iPATH Agility Controller integrity.

4.4.4.1 Upgrading (or downgrading) iPATH Agility Controller firmware

In certain circumstances it may be necessary to upgrade or downgrade the firmware of an iPATH Agility Controller to take advantage of particular features. The Upgrade iPATH Software option changes the firmware without affecting configuration data such as devices, channels, presets, users, groups and logs.

Note: Although configuration details are not affected during the firmware upgrade process, you are recommended to take a backup onto an external device before starting the upgrade process.

Note: When changing the iPATH Agility Controller firmware, it will be necessary to reboot the unit in order to apply the changes.

To upgrade/downgrade the iPATH Agility Controller firmware

1 Download the appropriate firmware file from Black Box technical support.

2 Visit the Dashboard > Updates page of the iPATH Agility Controller unit and within the 'Upgrade iPATH Software' section, click the Browse... button to locate the downloaded firmware file.

3 When you are ready to proceed, click the Upload button. The file will be uploaded, checked and applied to the secondary partition within the iPATH Agility Controller. A confirmation message will be displayed and you will also be prompted to reboot the iPATH Agility Controller.

4 When it is appropriate to do so (dependent on the current activity of the iPATH Agility Controller), click OK and then click the Reboot Now button. The iPATH Agility Controller will reboot using the new firmware partition.

Reset iPATH Configuration

This option can be used to reset iPATH Agility Controller to its initial configuration or a previous upgrade. When the iPATH Agility Controller server is reset, all devices, channels, presets, users, groups and logs will be removed. *Note: You are recommended to take a backup onto an external device before starting the upgrade process.*

If one or more previous upgrades have been installed on this system, you will be given the option to choose either the original factory image or the last upgrade image. They will be listed by version number - click the appropriate radio button to select.

Two other options are available within this section:

• *Also reset the server IP address* - When ticked, the IP address will be reset to the default: **169.254.1.3** and you will be reminded to manually navigate to that address.

• *Also delete security certificates and keys* - When ticked, all certificates and keys held within the server will be removed.

When the required options have been chosen, click the **Reset iPATH Configuration** button to commence.

Upload New TX/RX Firmware

Allows you to upload a firmware file to the iPATH Agility Controller server, which can then be used to upgrade Agility TX and RX units.

Install Firmware onto Devices

Allows you to determine various upgrade settings and then commence the upgrade process.

Please see **Upgrading Agility firmware globally** on the next page.

4.4.4.2 Upgrading Agility firmware globally

This method allows the iPATH Agility Controller admin user to upgrade firmware on receivers and transmitters, wherever they are located.

1 Use the "Upload New TX/RX Firmware" section to place new transmitter and/or receiver firmware file(s) onto the iPATH Agility Controller. Once uploaded, the stored firmware files are listed within the relevant "Available firmware" drop-down boxes within the sections below.

2 Within the "Install Firmware onto Devices" section, choose the Device Version (Agility standard or dual model), Device Type (RX or TX) and Firmware Type (Main or Backup copies).

3 Click the Available firmware drop-down box and select the required new firmware version.

   Note: There is no longer any support for the original Agility ACR1000A units within iPATH firmware version 4.1 onwards.

4 Click the "Install" button to apply the chosen firmware to the devices.

5 On the right side of the list, you can:

   • Individually select the devices to which the firmware upgrade will be applied by checking the "Upgrade" boxes next to each device, or

   • Use the "Upgrade All" option to apply firmware globally to all devices.

   • You are recommended to tick the "Reboot First" (or "Reboot All First" when using the "Upgrade All" option).

6 Click the "Upgrade Selected..." button to create a queue of devices to be upgraded. If there are many devices to upgrade, this may take some time.

   The status of devices during the upgrade process should be shown in near-real time on the receivers/transmitters pages and on the device's own page. The page will show whether the device is still in the queue to be upgraded or if it is in the process of rebooting with the new firmware. Note that the process of applying firmware to a device and enacting a reboot takes several minutes to complete.

4.4.5 Dashboard > Active Connections Page

Shows only connections that are currently active within the iPATH Agility Controller network. Please refer to the Connection Log page section below.

4.4.6 Dashboard > Connection Log Page

Shows all connections that have occurred within the iPATH Agility Controller network. The most recent connections are shown at the top, and the log is paginated (the number of rows per page can be set from the Dashboard > Settings page). The log can be filtered to show all connections, or only currently active connections. Current connections have no "end time" and a disconnect icon (🪓).

The "Audio Broadcast IP" and "Video Broadcast IP" columns show whether the audio and video are being sent directly from the transmitter to the receiver or broadcast to a multicast group. Direct links are denoted by the receiver's IP address only; whereas multicast broadcasts are indicated by the multicast icon (🖧) and the common multicast IP address (the address will be in the range specified within the "Multicast IP Address" option of the Dashboard > Settings page).

Actions that you can take within this page include:

• Hover the mouse over the receiver, user or channel names to show more information about each item.

• Hover the mouse over the five "Info" icons to see descriptions (audio on/off; video on/off; USB on/off; shared/exclusive mode; serial on/off).

• Click 🪓 to end a connection between a receiver and a channel.

4.4.7 Dashboard > Event Log Page

This page lists events that have occurred within the iPATH Agility Controller system. A row of buttons just below the blue options bar allows you to filter log page entries to show only particular categories, as follows:

All l Admin l Users l Login l Channel Changes l Device Status

Where:

- **All**: Lists all events

- **Admin**: Lists automatic events and/or those performed by the admin user (including: backup, scheduled backup, backup restored, updating iPATH Agility Controller settings, adding/removing/updating channels/users/devices, Active Directory Sync, Firmware upgrades, iPATH Agility Controller upgrades, etc).

- **Users**: Lists events performed by regular users (including: login, logout, channel connections, disconnects, etc).

- **Login**: Lists login and logout events, whether performed via the admin console or receiver devices.

- **Channel Changes**: Lists only channel changes (connections & disconnects).

- **Device Status**: Lists new devices that are added to the iPATH Agility Controller network, get restarted/rebooted or go online/offline

You can archive Event Log data to a CSV file via the "Archive log data" link that jumps to the relevant section within the Dashboard > Backups page.

4.4.8 Dashboard > Remote Support page

The remote support feature grants a member of the technical support team remote access to the iPATH Agility Controller unit. This page shows the current state of remote support, whether currently enabled or disabled, plus a button to change the remote support state.

Note: Before enabling remote support contact Black Box technical support.

4.5 The Channels Tab

The Channels tab provides access to all settings and options related directly to the video, audio and USB streams, collectively known as channels, emanating from any number of transmitters.

Click the CHANNELS tab to view the initial View Channels page.

The various other Channels pages (e.g. Add Channel, View Channel Groups, etc.) are selectable within the blue section located just below the tabs.

4.5.1 Search Filters

The key fields (Name, Description, and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click 🔍 to start the search. Optionally, use the ⊙ ⊙ buttons to invert the order of the listing.

The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click 🔍 again).

4.5.2 Channels > View Channels Page

This page lists all channels that currently exist within the iPATH Agility Controller system. A channel is automatically created for every transmitter when it is added and configured within the iPATH Agility Controller network. The new default channel for each added transmitter will inherit the name of the transmitter. Such default names can be altered at any time and additionally, you can also create new channels manually, if necessary.

Within the list of channels, the Allowed Connections column indicates how each channel may be accessed by users. By default, these settings are inherited from the global setting (configurable within the Dashboard > Settings page), however, each channel can be altered as required. The icons denote the following connection rules:

⊞ Connection details inherited from the global setting

👁 Video-Only

⌇ Shared

🔒 Exclusive

🔒 Private

The Channel Groups column shows to how many channel groups each channel belongs.

The Users column indicates how many users have permission to view each channel.

Actions that you can take within this page include:

- **Create a new channel**: Click the "Add Channel" option.

- **Create a new channel group**: Click the "Add Channel Group" option.

- **Configure an existing channel**: Click 🖉 for the required channel.

- **Clone an existing channel**: Click 📋 to use the settings for the current channel as the basis for a new channel entry.

- **Delete a channel**: Click ⊖ for the required channel.

- **Delete multiple channels**: Click the "Turn Batch Delete Mode On" button, the ⊖ icons for all channels are replaced with tick boxes. Tick the boxes of the channels that need to be deleted and then click the "Delete selected channels" button which appears at the bottom of the page. When you are finished, click the "Turn Batch Delete Mode Off" button.

- **View a channel group**: Click the "View Channel Groups" button.

4.5.3 Channels > Add or Configure a Channel

From the View Channels page, you can add a new channel or configure an existing channel:

- To create a new channel: Click the "Add Channel" option.

- To configure an existing channel: Click 🖉 for a channel.

The Add and Configure pages are similar in content.

Channel Name, Description and Location

These are all useful ways for you to identify the channel and its origins. A consistent naming and description policy is particularly useful in large installations.

Video, Audio, USB and Serial

These drop down boxes list all of the available streams from installed transmitters. When creating a channel, you can choose to take all four streams from the same transmitter or from different ones, as required.

Note: Where necessary, channels can be created without video, audio, USB and/or serial. Only one receiver can use a transmitter's serial port at any time.

Allowed Connection

This section allows you to define the types of connection that you wish to permit users to make. You can define particular individual or combined connection types to suit requirements.

Note: This setting for each channel acts as the final arbiter of whether exclusive access can actually be achieved. If you deny exclusive access rights within this setting, then exclusive access for any user cannot take place for this channel, regardless of settings made elsewhere.

- **Inherit from global setting** - uses the setting of the "Allowed Connection Modes" option within the Dashboard > Settings page.

- 👁 **Video-Only**: Allows users only to view the video output, the USB channel is denied.

- 🔗 **Shared**: Allows users to control a system in conjunction with other users.

- 🔒 **Exclusive**: Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.

- 🔓 **Private**: Allows a user to gain private access to a system, while locking out all others.

Group Membership

Groups provide a quick and easy way to manage settings for channels. By making a channel part of a particular group, the channel automatically inherits the key settings of that group.

The group membership section displays existing channel groups in the left list (to which the current channel does not belong) and the channel groups in the right list to which it does belong.

To add the channel to groups: Highlight one or more (use the CTRL key if selecting more than one) group names in the left list and then click ▶ to add the name(s) to the right list.

Note: You can also include or exclude individual channels by double clicking on them.

To add the channel to all groups: Click ▶▶ to move all group names from the left to the right list.

To remove the channel from groups: Highlight one or more (use the CTRL key if selecting more than one) group names in the right list and then click ◀ to move the name(s) back to the left list.

To remove the channel from all groups: Click ◀◀ to move all group names from the right to the left list.

Permissions

This section allows you to determine which users and user groups should be given access to this channel. Individual users and user groups are handled within separate sub-sections, but both use the same method for inclusion and exclusion.

To include one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the left list and then click ▶ to add them to the right list.

To include all users (or groups): Click ▶▶ to move all user/group names from the left to the right list.

To remove one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the right list and then click ◀ to move them back to the left list.

To remove all users (or groups): Click ◀◀ to move all user/group names from the right to the left list.

4.5.4 Channels > Add or Configure Channel Group

Channel groups allow easy permission-granting for several channels at once. Permissions can be set to determine which users can access channels within a channel group.

From the View Channels page, you can add a new channel group or configure an existing channel group:

• To create a new channel: Click the "Add Channel Group" option.

• To configure an existing channel: Click "the View Channel Groups" option and then click 🖊 for a group.

The Add and Configure Channel Group pages are similar in content.

Channel Group and Description
These are all useful ways for you to identify the channel and its origins. A consistent naming and description policy is particularly useful in large installations.

Channel Group Membership
Allows you to determine which channels should be members of the group. By making a channel part of the group, each channel automatically inherits the key settings of the group.

To add a channel to the group: Highlight one or more (use the CTRL key if selecting more than one) channel names in the left list and then click ⊙ to add the name(s) to the right list.

Note: You can also include or exclude individual channels by double clicking on them.

To add all channels to the group: Click ⊙ to move all channel names from the left to the right list.

To remove a channel from the group: Highlight one or more (use the CTRL key if selecting more than one) channel names in the right list and then click ⊙ to move the name(s) back to the left list.

To remove all channels from the group: Click ⊙ to move all channel names from the right to the left list.

Permissions
This section allows you to determine which users and user groups should be given access to channels within this group. Individual users and user groups are handled within separate sub-sections, but both use the same method for inclusion and exclusion.

To include one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the left list and then click ⊙ to add them to the right list.

To include all users (or groups): Click ⊙ to move all user/group names from the left to the right list.

To remove one or more users (or groups): Highlight one or more (use the CTRL key if selecting more than one) user/group names in the right list and then click ⊙ to move them back to the left list.

To remove all users (or groups): Click ⊙ to move all user/group names from the right to the left list.

4.6 The Receivers Tab

The Receivers tab shows a paginated table of all receiver devices within the iPATH Agility Controller network.

Click the RECEIVERS tab to view the initial View Receivers page.

The other Receivers pages (e.g. View Receiver Groups, Add Receiver Group, etc.) are selectable within the blue section located just below the tabs.

4.6.1 Search Filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click 🔍 to start the search. Optionally use the ⬆️ ⬇️ buttons to invert the order of the listing.

The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click 🔍 again).

4.6.2 Receivers > View Receivers

The table shows the following information for each receiver:

- Name
- IP address
- Description & Location

- Online status
- Firmware revision of receiver unit
- Manage (admin options - see below)

The Manage icons are as follows:

(Note: You can hover your mouse pointer over any icons to reveal additional information)

🖊️ **Configure device**: Displays the "Configure Receiver" page.

🔄 **Reboot device**: Allows you to reboot or reset a unit to its factory settings. A popup will ask which task you wish to carry out. A reboot is useful if a device enters an unknown state. A reset will return the unit to its factory default state and reset its IP address (the unit will retain any firmware updates that have been applied).

💡 **Identify unit**: Causes the LED lights to flash on the front of the selected unit. An alert will be shown if the unit cannot be contacted (e.g. if it is offline)

⛔ **Delete device**: Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work withthe iPATH Agility Controller.

🔌 **Connect to a channel**: A list of available channels is shown, along with connection modes (Video-Only/Shared/Exclusive/Private). The admin user can thus remotely change channel on any receiver.

🔌 **Disconnect**: If a receiver is currently connected to a channel, clicking the disconnect icon will end the connection, regardless of who is connected. Hovering over the icon will show which user is connected, which channel they are connected to, and when the connection was created.

877-877-2269 l blackbox.com

4.6.3 Receivers > Configure Receiver

From the View Receivers page, you can configure details for a receiver:

- Click 🖉 for a receiver.

Note: If the IP address of the receiver is changed, the device will need to reboot itself.

Device ID / Type - Identity of the receiver.

Online? - Current status.

MAC Address / 2 - Lists the fixed network identifiers for the single or double ports.

Main/Backup Firmware - The current firmware versions contained within the unit.

IP Address 2 - Lists the single or dual IP addresses for the unit. If the DHCP options are ticked then the fields will be grayed out.

Device Name, Description and Location
These are all useful ways for you to identify the receiver and its origins. A consistent naming and description policy is particularly useful in large installations.

Login Required
- **No**: When selected, anyone can use a receiver terminal and connect to a channel. The channels/permissions displayed to this anonymous user are those that are set for the "anonymous user" that is defined within the Dashboard > Settings page.

- **Inherit from Receiver Groups**: When selected, the requirement for user login will be determined by the "Login Required" settings within the Receiver Groups to which this unit belongs:

  - If ANY of the receiver groups (to which this receiver belongs) are set as "Login Required = Yes", this receiver will require login.

  - If ANY of the receiver groups (to which this receiver belongs) are set as "Login Required = Inherit..." and the global setting is "login required = yes", then this receiver will require login.

  - If ALL receiver groups (to which this receiver belongs) are set as "Login Required = No", then this receiver will NOT require login.

- **Yes**: When selected, a user will need to login with the username and password defined in the "Users" section. They will only be allowed to login if they have been granted permission to access that particular receiver.

Receiver OSD Alerts
Determine the required setting for pop up OSD alerts: Inherit, No or Yes.

Keyboard Country
Select the country code of the keyboard connected to the receiver.

Audio Input Type
Select the required audio input type.

Video Compatibility Check
This reads the EDID from the attached monitor and determines whether the monitor is capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out because a dual link resolution has been selected to display on a single link monitor.

Force 60Hz
If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (next page) cannot be altered when this option is enabled.

Video switching

Provides two options for video switching:

- Fast Switching (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.

- Match Frame Rate - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@60Hz and 1920x1080@50Hz then this setting will change the frame rate from 60Hz to 50 Hz every time that you switch.

Group Membership

To facilitate collective permission-granting for numerous receivers, a receiver can belong to one or more receiver groups. Any permissions applied to the receiver group are inherited by all receivers that are included within the receiver group. For example, multiple receivers can be made available to a user by placing them all in a receiver group and then granting the user permission to use that receiver group.

Permissions

This is hidden by default as, by default, all users have access to all receivers. You can deny access to particular receivers for a user in this section. However, be aware that users who are included within user groups may have access to the same receivers via their groups.

USB Settings

HID only

If enabled, allows only HID (mice and keyboards) devices to be connected to the receivers.

Disable Isochronous Endpoint Alerts

When an isochronous USB device is connected to the receiver there will no longer be a warning message. Agility units do not support isochronous devices.

Enable Isochronous Endpoint Attach

Some USB devices combine many USB devices behind a USB hub. e.g a keyboard with audio support. By enabling this option, devices will be allowed to connect to Agility receivers, however, the isochronous part (e.g. the audio component) of the devices will not work.

Advanced Port

This section allows you to determine USB port behaviour for use with certain USB devices.

The default is no reserved ports, Merging enabled and no feature code (or Quirk) set. It is recommended that these are left at the default settings and are only changed under advice from a technical support engineer.

For each of the four USB ports on the receiver, certain rules can be applied depending upon the USB device connected.

If you have reserved USB ports on the transmitter, you can select which USB port to use for a particular device.

You can turn off USB merging for a particular port. This will slow down switching as the USB device will be enumerated every time that you switch.

You can also enter an advanced feature if it is necessary for your USB device. The drop down lists the feature codes for some known USB devices. Otherwise please contact your local technical support agent for advice.

4.6.4 Receivers > Add Receiver Group or Configure Group

From the View Receiver Groups page, you can create a new group or configure an existing group:

- To create a new group: Click the "Add Receiver Group" option.

- To configure an existing group: Click 🖉 for a group.

The Add and Configure pages are similar in content.

Login Required
- **No**: When selected, anyone can use a receiver terminal and connect to a channel. The channels/permissions displayed to this anonymous user are those that are set for the "anonymous user" defined within the Dashboard > Settings page.

- **Inherit from global setting**: When selected, the requirement for user login will be determined by the "Login Required" setting within the Dashboard > Settings page.

- **Yes**: When selected, a user will need to login with the username and password defined in the "Users" section. They will only be allowed to login if they have been granted permission to access devices in the receiver group.

Enable Receiver OSD Alerts
Determine the required setting for pop up OSD alerts: Inherit, No or Yes.

The next fields are the USB settings.

Note: USB port reservation and advanced USB features will be added to future releases of the iPATH Agility Controller management system.

Enable Video Compatibility Check
This reads the EDID from the attached monitor and determines whether the monitor is capable of displaying the selected video mode before connecting a channel. This prevents the receiver showing a black screen and the user being locked out because a dual link resolution has been selected to display on a single link monitor.

Force 60Hz
If enabled, the receiver frame rate is held at 60Hz regardless of the video input frame rate. The Video Switching options (below) cannot be altered when this option is enabled.

Video switching
Provides two options for video switching:

- Fast Switching (default state) - Retains the same frame rate (at either 50Hz or 60Hz) depending upon which video resolution was displayed first.

- Match Frame Rate - Follows the source frame rate and will change the frame rate every time this changes even if the video resolution doesn't change. If you have one receiver switching between 1920x1080@60Hz and 1920x1080@50Hz then this setting will change the frame rate from 60Hz to 50 Hz every time that you switch.

USB Settings
See previous page.

Group Membership

This section allows you to easily include or exclude individual receivers for this group. All relevant group permissions will be applied to all receivers that are included within the group. Receivers that are not currently included in this group within the left list and those receivers that are included within the right list.

To add a receiver to this group: Highlight one or more (use the CTRL key if selecting more than one) receiver names in the left list and then click ⊙ to add the name(s) to the right list.

To add all receivers to the group: Click ⊙ to move all receiver names from the left to the right list.

To remove a receiver from the group: Highlight one or more (use the CTRL key if selecting more than one) receiver names in the right list and then click ⊙ to move the name(s) back to the left list.

To remove all receivers from the group: Click ⊙ to move all receiver names from the right to the left list.

Permissions

This is hidden by default because all users have access to all receivers. You can deny access to the receiver group, however, be aware that users who are included within user groups may have been given access to the receiver group via their user groups.

4.6.5 Receivers > Update Firmware

Click this option to go straight to the Dashboard > Updates page. See Dashboard > Updates page for more details.

4.7 The Transmitters Tab

The Transmitters tab shows a paginated table of all transmitter devices within the iPATH Agility Controller network.

Click the TRANSMITTERS tab to view the transmitters page.

4.7.1 Search filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click 🔍 to start the search. Optionally use the ⬆ ⬇ buttons to invert the order of the listing.

The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "mac" in the name, and "mixed" in the description). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter, (you can also empty the search box and click 🔍 again).

4.7.2 Transmitters > View Transmitters Page

The table shows the following information for each receiver:

- Type (transmitter type)

- Name
- Online status

- IP address
- Firmware revision of transmitter

- Channels (attributed to each transmitter)
- Presets

- Description & Location
- Manage (admin options - see below)

The Manage icons are as follows:

(Note: You can hover your mouse pointer over any icons to reveal additional information)

✏ **Configure device**: Displays the "Configure Transmitter" page.

🔄 **Reboot device**: Allows you to reboot or reset a unit to its factory settings. A popup will ask which task you wish to carry out. A reboot is useful if a device enters an unknown state. A reset will return the unit to its factory default state and reset its IP address (the unit will retain any firmware updates that have been applied).

💡 **Identify unit**: Causes the LED lights to flash on the front of the selected unit. An alert will be shown if the unit cannot be contacted (e.g. if it is offline).

⊖ **Delete device**: Confirmation will be requested. You will need to factory-reset any devices that you wish to re-configure to work with the iPATH Agility Controller.

4.7.3 Transmitters > Configure Transmitter

When you click 🖊 for a particular transmitter, this page lists information about the unit and allows numerous settings to be configured.

IP Address

Allows you to alter the IP address of the transmitter unit. Any change in address will be enacted when you click the "Save" button at the foot of the page. Any IP connections currently made to the transmitter will be ended.

Device Name, Description and Location

These are useful identifiers for the transmitter unit and its exact location. These become even more valuable as the number of transmitters within the system increases.

Enable Dummy Boot Keyboard

It is often necessary to have a keyboard reported at start up. This setting means that a "Virtual Keyboard" is always reported to the USB host. It may be necessary to disable this for use with some KVM switches.

USB Speed

Select Low/full speed or High speed USB operation.

USB Hub Size

Select either a 13 or 7 port USB hub. This determines the number of USB devices that can be connected to a single Transmitter.

Peak Bandwidth Limiter

The transmitter will use as much of the available network bandwidth as necessary to achieve optimal data quality, although typically the transmitter will use considerably less than the maximum available. In order to prevent the transmitter from 'hogging' too much of the network capacity, you can reduce this setting to place a tighter limit on the maximum bandwidth permissible to the transmitter. Range: 1 to 95%.

Video Settings

This section allows you to directly adjust various key video controls within the transmitter in order to obtain the most efficient operation taking into account connection speeds and the nature of the video images sent by that transmitter.

Magic Eye

Determines whether the Magic Eye feature should be enabled on Agility (not Agility revision 1) transmitters. Magic Eye works to overcome the issues with increased bandwidth usage caused by 'dithering' techniques used on some computers, such as Apple Macs. See the Agility Dual user guide for more details.

DDC

Determines whether video configuration details should be harvested from connected display screens or a static fixed EDID report should be used. Care must be taken when selecting a Dual Link Video resolution as only Agility Dual units support a Dual Link Video resolutions. In the case of a Dual Link EDID being set in the Global settings, no EDID will be set on Video port 2 of the Agility Dual transmitters.

EDID optimisation

When this option is ticked, the Transmitters will compare the native resolution settings of their monitors when switching. If the monitor has the same native resolution as the previous one, the new EDID is not sent to the graphics card. This speeds up switching as the graphics card does not have to go through a hotplug detect routine when a new receiver is switched to that channel. If the new receiver has a monitor with a different native resolution, then the EDID will be updated to allow for a change in video mode.

Hot Plug Detect Control

Determines whether to enable hot plug detection for monitors. By default this is enabled.

Hot Plug Detect Signal Period

By default this is set at 100ms, which is sufficient for most graphics cards. Occasionally it may be necessary to adjust this. A technical support engineer will advise if necessary.

Background Refresh

The transmitter sends portions of the video image only when they change. In order to give the best user experience, the transmitter also sends the whole video image, at a lower frame rate, in the background. The Background Refresh parameter controls the rate at which this background image is sent. The default value is 'every 32 frames', meaning that a full frame is sent in the background every 32 frames. Reducing this to 'every 64 frames' or more will reduce the amount of bandwidth that the transmitter consumes. On a high-traffic network this parameter should be reduced in this way to improve overall system performance. Options: Every 32 frames, Every 64 frames, Every 128 frames, Every 256 frames or Disabled.

Frame Skipping

Frame Skipping involves 'missing out' video frames between those captured by the transmitter. For video sources that update only infrequently or for those that update very frequently but where high fidelity is not required, frame skipping is a good strategy for reducing the overall bandwidth consumed by the system. Range: 0 to 99%.

Serial Settings

Serial Parity, Serial Data Bits, Serial Stop Bits, Serial Speed

This group of settings allows you to define the key parameters for the AUX port of the transmitter so that it matches the operation of the device attached to it.

4.7.4 Transmitters > Update Firmware

Click this option to go straight to the Dashboard > Updates page. See Dashboard > Updates page for more details.

4.7.5 Transmitters > Configure New Transmitter

This page is displayed whenever a new transmitter is added to the network.

The IP Address 1 field, showing 0.0.0.0, is for an unconfigured device on its zero config address. Before the iPATH Agility Controller can add the device into its database, a new IP address must be added to IP Address 1. This is the system IP address and applies equally for Agility and Agility Dual models.

Agility Dual units have a Teaming port which provides a second 1Gigabyte link port which can be used for bandwidth doubling and/or redundancy. The IP address 2 field is for the Teaming port. In order to use the Teaming port, IP address 2 field must be given a valid IP address. For Agility units, this field will remain blank.

4.8 The Servers tab

The Servers tab shows a table of all servers within the iPATH Agility Controller network.

Click the SERVERS tab to view the page.

For installations that require greater redundancy, it is possible to have two iPATH Agility Controllers running on the same subnet. If used on multiple subnets it is possible to have two or more servers on each subnet. If the primary server fails then a secondary server with the same database can take over until the primary unit recovers.

Each server entry will have one of four possible states within the Rôle column:

• Unconfigured The server is a factory fresh device or has performed a full factory reset. This does not yet have a proper role.

• Solo   This is a server acting as a standalone iPATH Agility Controller. If there is only going to be one iPATH Agility Controller on the subnet, this is the Rôle that should be used.

• Primary The server is configured as a fully functional iPATH Agility Controller from which a back-up server can be slaved.

• BackUp This server is configured to serve as a back up to the Primary.

Each server entry will also show one of six entries within the Status column:

• Active This server is functioning as an iPATH Agility Controller and is administering Agility devices. Primary or Solo servers with this status are fully functional iPATH Agility Controllers that will accept network configuration changes. A backup server with this status is functioning as an Active Primary. It will execute channel changes, but will not accept network configuration changes.

• Standby This server is currently maintaining its database as a copy of the primary in readiness to take over if necessary.

• Offline This server should be maintaining a copy of the primary's database, but is not doing so.

• Initialising This is the initial status upon start up. This should not persist beyond the initial start up procedure.

• Quiescent This is an inactive server on the network. It will not function without remedial action from its system administration. A typical reason for this is the presence of another server on the network blocking its configured role. i.e. two servers are configured as a primary on the same subnet.

• Failed This server has suffered a serious internal failure.

4.8.1 Servers > Configure Server

When you click 🖉 for a particular server, this page lists information about the unit and allows several basic settings to be configured.

Rôle
Allows you to change the server's function between primary and solo (see descriptions above).

Device Name, Description and Location
These are useful identifiers for the server unit and its exact location. These become even more valuable as the number of servers within the system increases.

For details about setting up server redundancy, please see Appendix C - Redundant servers: Setting up and swapping out.

4.9 The Users Tab

The Users tab shows a paginated table of all users within the iPATH Agility Controller network. Within the list, the admin user is always present and cannot be deleted - to avoid being locked out of the iPATH Agility Controller system. The username and name details of the admin account, however, can be edited as required.

Click the USERS tab to view the initial View Users page.

The other user pages (e.g. Add User, View User Groups, etc.) are selectable within the blue section located just below the tabs.

4.9.1 Search Filters

The key fields (Name, Description and Location) all provide a search filter to locate particular items within long lists. Enter a full or partial search string into the appropriate filter box and then click 🔍 to start the search. Optionally use the ⊙ ⊙ buttons to invert the order of the listing.

The page will reload with the same pagination/sort order, but with the added search filter. It's possible to filter by several columns at once (e.g. search for all entries with "B" in the Username, and "Smith" in the Last Name). Search terms are case-insensitive. You can re-sort and paginate on filtered results without losing the filters.

To remove a filter, click the red cross next to the relevant filter (you can also empty the search box and click 🔍 again).

4.9.2 Users > View Users Page

The table shows the following information for each user:

• AD - indicates whether the user was imported from Active Directory

• Username   • First Name   • Last Name

• User Groups - the number of user groups to which the user belongs

• Channels - the number of channels to which the user has access

• Receivers - the number of receivers to which the user has access

• Allow Private? - indicates whether the user is permitted to access channels in private mode (✔ - Yes, ✖ - No, ⛫ - Inherited setting from user groups)

• Suspended - indicates the user account status (✔ - User is suspended, ✖ - User account is active, i.e. not suspended)

• Admin - indicates whether the user has admin privileges

The Edit option icons are as follows:

🖉 **Configure user**: Displays the "Configure User" page.

📋 **Clone user:** Create a complete copy of the currently selected user entry.

⊖ **Delete user**: Confirmation will be requested.

4.9.3 Users > Add User or Configure User Page

From the View Users page, you can add a new user or configure an existing user:

- To add a user: Click the "Add User" option.

- To configure an existing user: Click 🖊 for a user.

The Add and Configure pages are similar in content.

Username
The username is mandatory and must be unique within the iPATH Agility Controller installation.

Note: If a user is synced with Active Directory, it is not possible to change the Username, First/Last Name, Password, or User Group membership. These items must be edited on the Active Directory server and the changes will filter through to the iPATH Agility Controller the next time a sync takes place with Active Directory.

First Name, Last Name and Email
The First Name, Last Names and Email address entries are optional but are advisable within an installation of any size or one that will be administered by more than one person.

Require Password
Determines whether the chosen user must enter a password to gain access to channels and/or iPATH Agility Controller admin system.

Password
The password is required for logging into a channel and/or for logging into the iPATH Agility Controller admin system, if the user is to be granted admin privileges.

iPATH Admininistrator?
When set to Yes, the user is granted privileges to login to the iPATH Agility Controller admin system and make changes.

Account Suspended?
Allows the admin user to temporarily prevent the user from logging in without the need to delete the whole account.

Allow Private Mode?
Defines whether the user is able to connect to channels privately (locking out other users during a session). When this is set to "Inherit from User Groups/Global Setting", if ANY user-group that a user is a member of is granted permission to connect exclusively, then the user will have permission to connect exclusively. *Note: It is an additional requirement that the channel being accessed by the user, must also permit exclusive access.*

Enable Remote OSD?
Supported in firmware v3.0 or greater. This option determines whether the chosen user should be permitted to use the remote OSD functionality which permits access to remote receivers in order to change channels or presets even though a user has not logged into those receivers. Please see Using the Remote OSD feature for details.

Group Membership
This section allows you to select which users should be members of the group. Any permissions applied to the user group are inherited by all users in the user group. Users who are not currently members are shown in the left list and those who are members are shown within the right list. See Including and excluding a user... on the right for details about including and excluding group membership.

Permissions
This section defines to which channels and/or channel groups the user within this group should have access. *Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.*

See **Including and excluding a user...** on the next page for details about including and excluding channels and/or channel groups.

Receiver and Receiver Group Permissions
Receiver and Receiver Group Permissions are hidden by default because all users are initially granted permission to use all receivers. If desired, permission to use a receiver and/or receiver group may be withdrawn from a user by revealing this section.

4.9.4 Users > Add User Group or Configure Group Page

From the View User Groups page, you can create a new group or configure an existing group:

- To create a new group: Click the "Add User Group" option.

- To configure an existing group: Click 🖊 for a group.

The Add and Configure pages are similar in content.

User Group Name
The User Group name must be unique within the iPATH Agility Controller installation.

Allow Private Mode?
Defines whether the users within the group will be able to connect to channels privately (locking out other users during the session). When this is set to "Inherit from global setting", the setting for the "Grant all users private access" option (within Dashboard > Settings) will be applied. *Note: The final arbiter of whether any user can gain private access is always whether the channel being accessed is also set to allow private connections.*

Enable Remote OSD?
Determines whether members of the chosen user group should be permitted to gain OSD access to remote receivers in order to change channels.

Group Membership
This section allows you to select which users should be members of the group. Any permissions applied to the user group are inherited by all users in the user group. Users who are not currently members are shown in the left list and those who are members are shown within the right list. See Including and excluding a user... below for details about including and excluding group membership.

Permissions
This section defines to which channels and/or channel groups the user within this group should have access. Note: Only the channels/channel groups for which a user is given permission to access will appear within their channel list.

See **Including and excluding a user...** below for details about including and excluding channels and/or channel groups.

Receiver and Receiver Group Permissions
Receiver and Receiver Group Permissions are hidden by default because all users/user groups are initially granted permission to use all receivers. If desired, permission to use a receiver and/or receiver group may be withdrawn from members of this user group by revealing this section.

4.9.4.1 Including and Excluding a User Within Groups or Channels

The Group Membership and Permissions section use the same method to determine inclusion and exclusion:

To add the user to a group or grant access to a channel: Highlight one or more (use the CTRL key if selecting more than one) of the entries in the left list and then click 🔘 to add them to the right list (you can also double-click on an entry to quickly add it).

To add the user to all groups or grant access to all channels: Click 🔘 to move all entries from the left to the right list.

To remove the user from a group or channel: Highlight one or more (use the CTRL key if selecting more than one) entries in the right list and then click 🔘 to move them back to the left list (you can also double-click on an entry to quickly remove it).

To remove the user from all groups or channels: Click 🔘 to move all entries from the right to the left list.

4.9.5 Users > Active Directory

To simplify integration alongside existing systems within organizations, iPATH Agility Controller can be synchronized with an LDAP/ Active Directory server. This allows a list of users (and user groups), together with usernames and group memberships to be quickly imported and kept up to date.

Initial configuration

The basic Active Directory (AD) server details are defined in the Dashboard > Settings page. Once configured, the Users > Active Directory page (called "Import Users from Active Directory") will allow you to scan the AD server for a list of folders and users/ groups within those folders.

Choosing users and groups

Once scanned, the "Import Users from Active Directory" page shows all folders that are available on the AD server.

1 Use the "Include Users" and "Include Groups" checkbox columns on the right hand side of the folder lists to select which items to import (with optional additional LDAP filters where necessary).

   - If an AD user was not in the iPATH Agility Controller user database, they will be imported.

   - If an AD user is already in the iPATH Agility Controller user database, they are kept.

   - If an AD user is NOT marked for import/sync from the AD import page, and they already exist in the iPATH Agility Controller user database, they will be removed from the iPATH Agility Controller user database during the sync operation.

     IMPORTANT: It is thus vital to ensure that all users you want in the iPATH Agility Controller system are always selected for import/sync, otherwise they will be removed.

2 Choose the required "Re-Synchronize" interval. Choices are Never, Hourly, Daily or Weekly.

3 You can choose to synchronize immediately or to preview the results of your settings:

   - Click the "Preview" button to view the list of users that will be added/updated/removed on this synchronization. Once previewed, you can either go ahead with the sync or return to the filter page and edit your settings.

   - Click the "Save & Sync" button to synchronize the selected items into the iPATH Agility Controller user database.

4.9.5.1 Active Directory Tips

- A backup schedule is recommended so that any changes on the AD server are carried across to the iPATH Agility Controller regularly. You can choose from hourly/daily or weekly syncs. The settings/filters saved on this screen will be applied to each subsequent sync, ensuring that your list of users is kept accurate.

- To temporarily remove a particular user from iPATH Agility Controller access, without having to make complicated LDAP filters, simply edit the iPATH Agility Controller user to be suspended (see Users > Add User or Configure User page). Even though they will continue to be imported/synced from AD, they will be prevented from logging on.

- All LDAP filters should be self-contained, e.g: (!(cn=a*))

- Be sure to save any changes made to the sync settings before clicking the "sync-now" option. Otherwise, the next scheduled sync operation will overwrite any user changes you made in your "sync-now".

- User groups are only imported from AD to iPATH Agility Controller if they contain users that are set to be imported too (i.e. a group will not be imported, even if it contains users, unless its users match the sync filters).

- Associations between users and user groups can only be made on the AD server - it is not possible to edit user/user-group membership for AD users/groups on the iPATH Agility Controller.

- Users and groups are technically "synchronized" rather than "imported" - each time a sync takes place, details are updated and if a user no longer matches the sync filters, they will be removed from the iPATH Agility Controller user list.

4.10 The Presets Tab

Presets enable multiple actions to be pre-defined so that they can be initiated with a single action. This feature is particularly useful when switching multiple Agility units, such as in the example below where multiple video heads need to be switched in unison between different server systems, as shown in Figure 4-2:
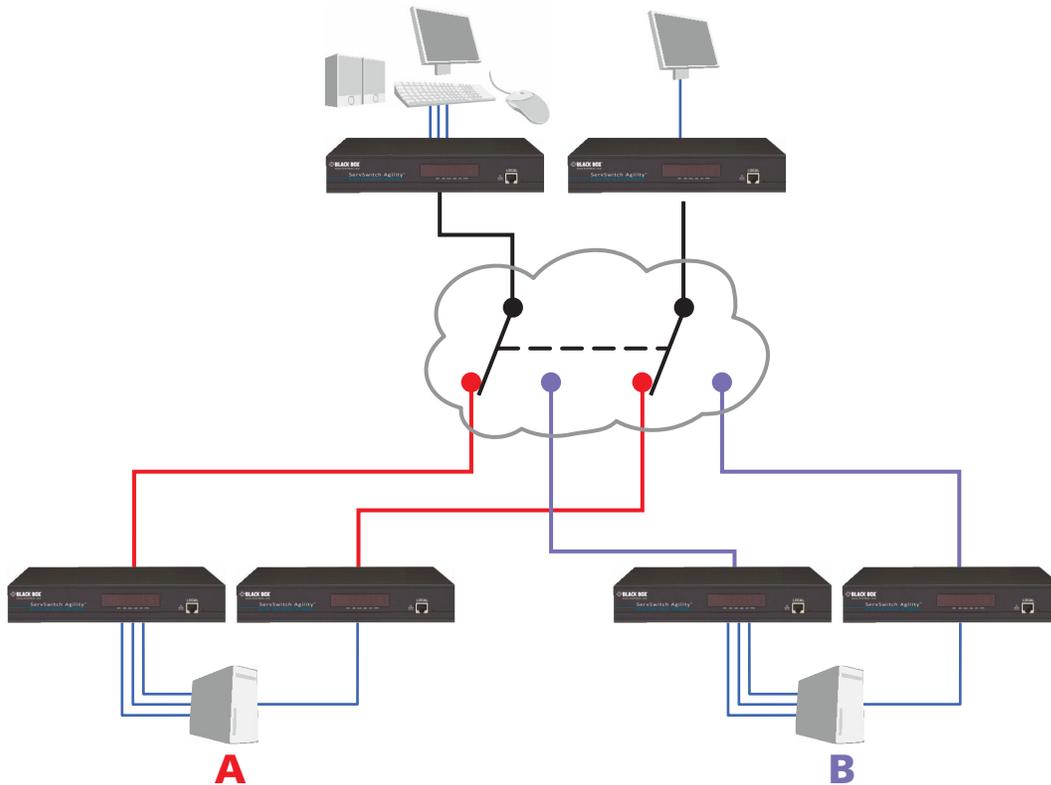
Figure 4-2. Preset switching allows multiple units to react in unison to a single action.

According to how a preset is configured, it is possible to have one or more receivers connected to separate channels (i.e. unicast) or multiple receivers connected to a single channel (i.e. multicast).

continued

The Presets page is where the admin user can create and configure new and existing presets.

Click the PRESETS tab to view the Presets page.

The nature of each preset, i.e. which receiver connects to which channel(s), is defined by the admin. The permitted connection modes are worked out according to:

- The topology of the preset,

  AND

- The current connections within the iPATH Agility Controller network.

For instance, if two receivers in a preset are configured to connect to the same channel (multicast), it will not be possible to connect to the preset in exclusive mode.

The presets table shows the preset name, description, allowed connection modes, and number of receiver-channel pairs in the preset.

If any preset-pairs are misconfigured (e.g. a channel no longer exists), a warning triangle will appear. The preset will NOT be usable if any receiver-channel pairs are misconfigured.

The admin user can connect any presets using the standard Video-Only/Shared/Exclusive/Private buttons.

Note: There are no permissions to set for a preset. Instead, a preset will only be available to users who have permission to use ALL receivers and channels within the preset. In other words, permissions on the preset are implied by the permissions on the preset's contents.

4.10.1 Presets > Add or Configure Presets Page

From the Presets page, you can add a new preset or configure an existing preset:

• To create a new preset: Click the "Add Preset" option.

• To configure an existing preset: Click 🖉 for a preset.

The Add and Configure pages are similar in content.

Preset Name and Description
The Preset Name is mandatory, whereas the Description is optional but recommended when numerous presets will be used. A consistent naming and description policy is particularly useful in large installations.

Receiver - Channel Pairs
Pair 1
From the two drop down lists, choose a receiver and a corresponding channel for it to connect with. This base pair can be altered but cannot be deleted from the preset.

Add another pair
Click this link to define another receiver/channel pairing.

Note: While channels can be assigned to multiple receivers, each receiver may only appear once within a single preset.

Allowed Connections
Choose one of the following connection rules to be applied to the preset:

• Inherit from global setting

• 👁 Video-Only

• ⮴ Shared

• 🔒 Exclusive

• 🔓 Private

Note: If multicasting is present (e.g. two or more receivers connected to the same channel or two channels containing the same audio/video end point), it will not be possible to choose the 'Private' connection mode.

4.11 The Statistics tab

The Statistics tab provides an opportunity to view a range of real-time data measurements related to any links within the iPATH Agility Controller network. This is particularly useful for optimization and troubleshooting purposes.

Click the STATISTICS tab to view the page.

To view statistics

1 To the right of the unit for which you wish to view statistics, click the dark graph icon (🖾) so that it gains a white background (🖾).

2 Click on the device name to display the available statistics.

A dynamic graph will be displayed showing the chosen data series for the selected Agility units.

5. Operation

For non-admin users, iPATH Agility Controller offers a clear way to choose and access multiple channels.

5.1 Logging In

1 On the keyboard connected to your Agility receiver, press the hotkey combination **Ctrl-Alt-C** to display the On-Screen Display or OSD (this hotkey combination can be altered on the Dashboard > Settings > Receivers page).

   You will either see the list of channels for which you have permission or be presented with the following login, as shown in Figure 5-1:
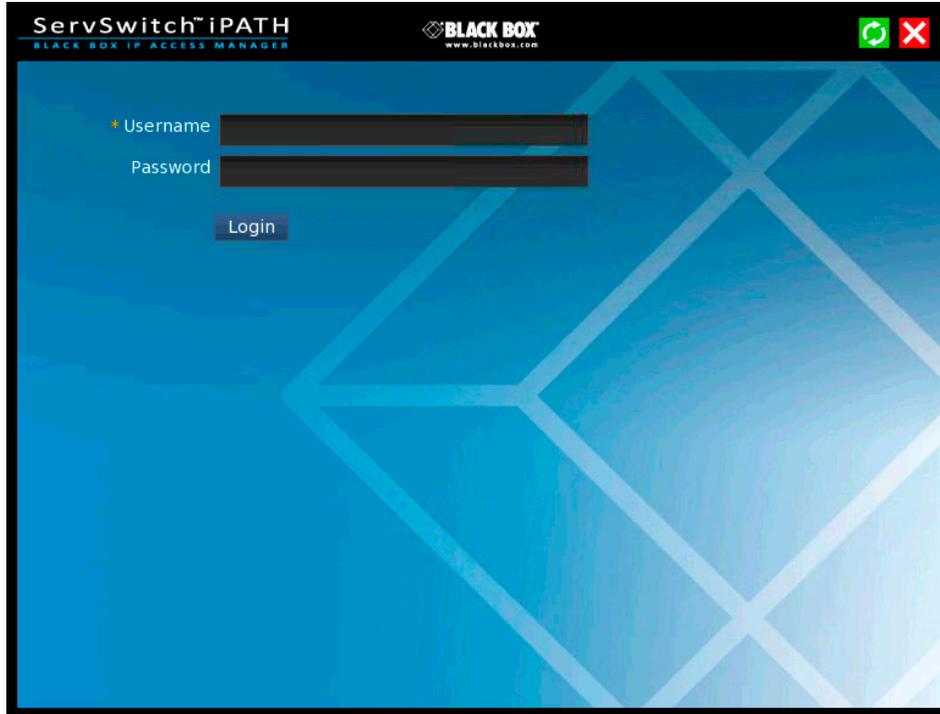

Figure 5-1. Login page.

2 Enter your Username and Password and click the Login button to display the local OSD screen.

   Once logged in, you will remain logged in until either you click the Logout link in the top right of the OSD; or there is no activity for two days or until the Agility unit is rebooted.

5.2 Hotkey shortcuts

The following standard shortcuts are available for use with the Local OSD (and Remote OSD). These default hotkey combinations can be altered within the Dashboard > Settings > Receivers page.

Left Ctrl + Left Alt + C:	Launch the OSD
Left Ctrl + Left Alt + X:	Disconnect the current receiver
Left Ctrl + Left Alt + 3:	Connect to the channel/preset saved in shortcut slot 3
Left Ctrl + Left Alt + A:	Re-connect to the last channel
Left Ctrl + Left Alt + V:	Change the current connection to the view-only mode
Left Ctrl + Left Alt + S:	Change the current connection to the shared mode
Left Ctrl + Left Alt + E:	Change the current connection to the exclusive mode
Left Ctrl + Left Alt + P:	Change the current connection to the private mode

5.2.1 Creating/using favorites and shortcuts

When the OSD contains many possible channels and presets, it can be useful to mark the most commonly visited ones as favorites. For those channels that you'd like to access by keyboard shortcut, there are also ten assignable hotkeys.

5.2.1.1 To create a new favorite

1 Click the ⭐ icon next to the required channel or preset.

2 Click the SAVE ⭐ button at the top of the page.

5.2.1.2 To display favorites

The star shown at the top of the channel list has three appearances to represent the three display modes. Click the star to change the mode:

⭐ Currently showing all channels/presets.

⭐ Currently showing only favorites.

⭐ Currently showing only numbered shortcuts.

5.2.1.3 To create a new hotkey shortcut

1 Click the ⭐ icon next to the required channel or preset. The screen will list the ten hotkey slots, with any available slots listed as EMPTY. Click the number prefix (from 1 to 0) of an available slot.

   Note: To remove a previous channel from a slot, click the ✖ icon on the right side of the slot.

2 You will now be asked to choose which mode should be used to access the channel when using this shortcut. Select View Only, Shared or Exclusive, as appropriate.

3 Click the SAVE ⭐ button at the top of the page. As mentioned above, you will now be able to access the chosen channel by using the hotkeys (Left Ctrl + Left Alt, as standard) plus the number that you assigned to it.

   The list of channels for which you have permission will be shown, as shown in Figure 5-2 on the next page.

5.3 The Local OSD screen

Once logged in, the list of channels for which you have permission are shown in the Local OSD (blue bars) screen.

- To choose a channel/preset, click on one of the blue connection icons (👁 ⬂ 🔒 🔓) shown to the right of the required channel/preset name (see the Connection buttons box below right).

- Where many channels/presets are listed, use the Channel Name and Description search boxes and list arrows to filter the choices.

- To use the Remote OSD feature, click the 🔸 icon in the top right corner.

Top corner icons

🔸	Enter 'Remote OSD' mode
❌	Exit 'Remote OSD' mode
❓	Display the help pages
🔄	Refresh the current page
❌	Close the OSD

Favorites icons

⭐	Currently showing all channels/presets
⭐	Currently showing only favorites
⭐	Currently showing only numbered shortcuts
⭐	Click to add this channel as a favorite
2	This channel is a numbered shortcut

Figure 5-2. Local OSD screen channels list.

Sorting icons

🖥	Currently showing channels and presets. Click to change
🖥	Currently showing only channels. Click to change
🖥	Currently showing only presets. Click to change
🔍	Filter this column using the specified term
❌	Remove the search filter
🔼	Click to sort the list in ascending order via this column
🔼	The list is sorted in ascending order via this column

Connection buttons

There are four connection modes:

👁	Video-Only:	Allows users only to view the video output, the USB channel is denied.
⬂	Shared:	Allows users to control a system in conjunction with other users.
🔒	Exclusive:	Grants exclusive control to one user while all others can simultaneously view and hear, but not control, the output.
🔓	Private:	Allows a user to gain private access to a system, while locking out all others.

Connection buttons shown in blue are ready to select. Icons in green have been selected by another user and those shown in gray are not available.

🔹 End this connection

5.4 Using the Remote OSD feature

The Remote OSD feature allows authorized users to access and take control of Agility receivers other than the one to which they are connected. Once linked in, users can then determine which channels the remote receivers should link with.

Remote OSD requires the following:

• The iPATH Agility Controller(s) and all Agility units must have firmware version 3.0 or greater.

• A user must have been given specific authorization to access one or more remote receivers.

5.4.1 To access the Remote OSD

1 On the keyboard connected to your Agility receiver, press the hotkey combination Ctrl-Alt-C to display the Local OSD login screen.

2 If required, enter your Username and Password and click the Login button.

3 In the top right corner, click the ⬦ icon.

4 The screen will list all of the receivers to which you have access rights. Click on the required receiver from the list:
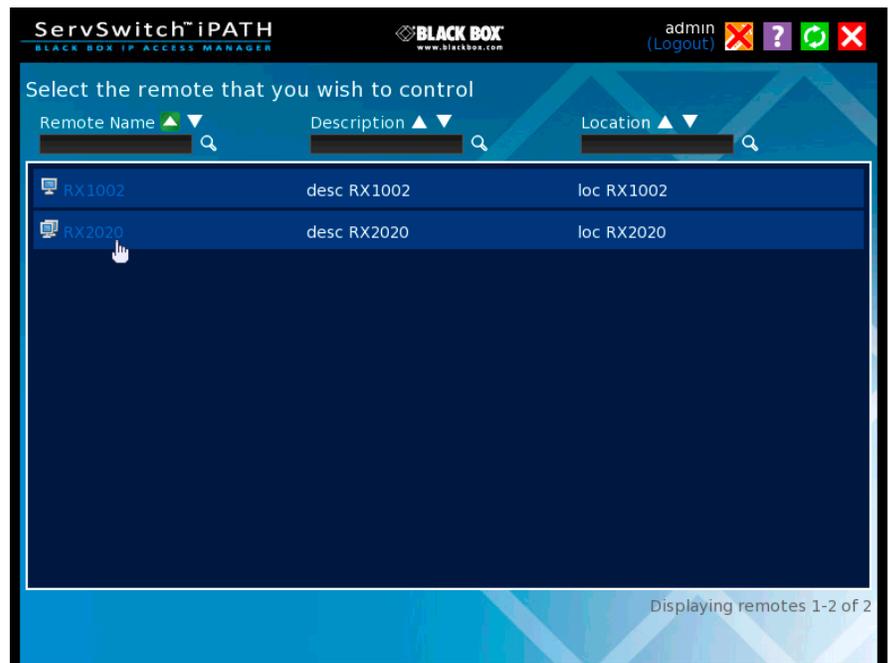
5 The Remote OSD for the chosen Agility receiver will be displayed. Remote OSDs always have black horizontal bars in the background to differentiate them from the standard local OSD:

6 The behavior of the controls is generally the same as for the Local OSD screen with the following exceptions:

• To avoid confusion, you cannot login or logout while in Remote OSD mode. Click the ✖ icon to first return to the Local OSD.

• Hotkeys will only affect the current receiver to which you are connected, not the remotely-controlled receiver.

7 To exit from the Remote OSD, click the ✖ icon in the top right corner.
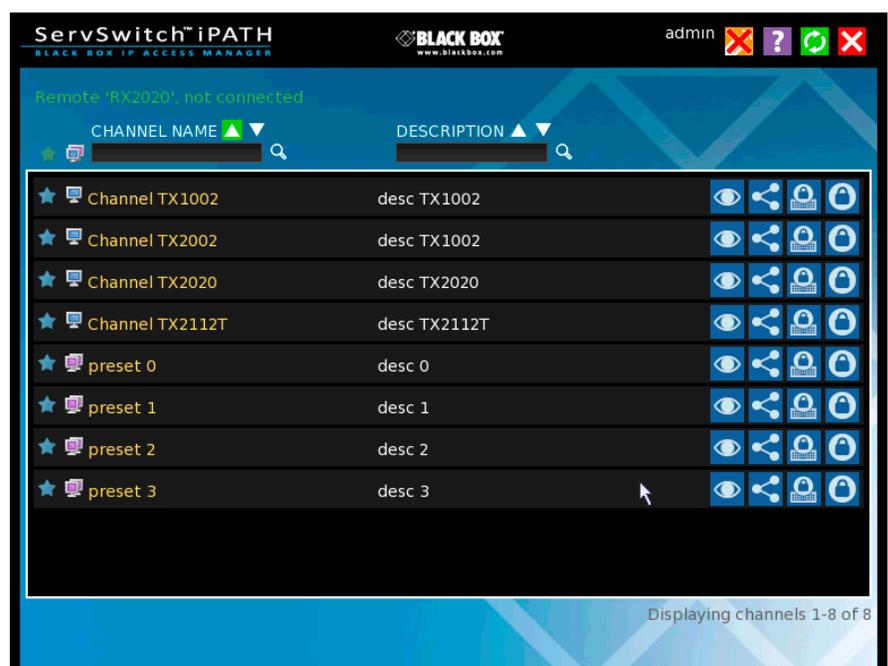
6. Further information

This chapter contains a variety of information, including the following:

- Appendix A - Tips for success when networking Agility units

- Appendix B - Troubleshooting

- Appendix C - Redundant servers: Setting up and swapping out

- Appendix D - Upgrade Licence

- Appendix E - Glossary

- Appendix F - iPATH API

- Safety information

Appendix A. Tips for success when networking Agility units

Agility units use multiple strategies to minimise the amount of data that they send across networks. However, data overheads can be quite high, particularly when very high resolution video is being transferred, so it is important to take steps to maximise network efficiency and help minimise data output. The tips given in this section have been proven to produce very beneficial results.

A.1 Summary of steps

• Choose the right kind of switch.

• Create an efficient network layout.

• Configure the switches and devices correctly.

A.2 Choosing the right switch

Layer 2 switches are what bind all of the hosts together in the subnet. However, they are all not created equally, so choose carefully. In particular look for the following:

• Gigabit (1000Mbps) or faster Ethernet ports,

• Support for IGMP v2 (or v3) snooping,

• Support for Jumbo frames up to 9216-byte size,

• High bandwidth connections between switches, preferably Fiber Channel.

• Look for switches that perform their most onerous tasks (e.g. IGMP snooping) using multiple dedicated processors (ASICS).

• Ensure the maximum number of concurrent 'snoopable groups' the switch can handle meets or exceeds the number of Agility transmitters that will be used to create multicast groups.

• Check the throughput of the switch: Full duplex, 1Gbps up- and down- stream speeds per port.

• Use the same switch make and model throughout a single subnet.

• You also need a Layer 3 switch. Ensure that it can operate efficiently as an IGMP Querier.

A.2.1 Layer 2 (and Layer 3) switches known to work

• Cisco 2960

• Cisco 3750

• Cisco 4500

• Cisco 6500

• Extreme Networks X480

• HP Procurve 2810

• HP Procurve 2910

• H3C 5120

• HuaWei Quidway s5328c-E1 (Layer 3)

A.3 Creating an efficient network layout

Network layout is vital. The use of IGMP snooping also introduces certain constraints, so take heed:

- Keep it flat. Use a basic line-cascade structure rather than a pyramid or tree arrangement (see note below).

- Keep the distances between the switches as short as possible.

- Ensure sufficient bandwidth between switches to eliminate bottlenecks.

- Where the iPATH Agility Controller manager is used to administer multiple Agility transceivers, ensure the iPATH Agility Controller manager and all Agility units reside in the same subnet.

- Do not use VGA to DVI converters, instead replace VGA video cards in older systems with suitable DVI replacements. Converters cause Agility local units to massively increase data output.

- Wherever possible, create a private network.

A.3.1 The recommended layout

The layout shown in Figure A-1 below has been found to provide the most efficient network layout for rapid throughput when using IGMP snooping:
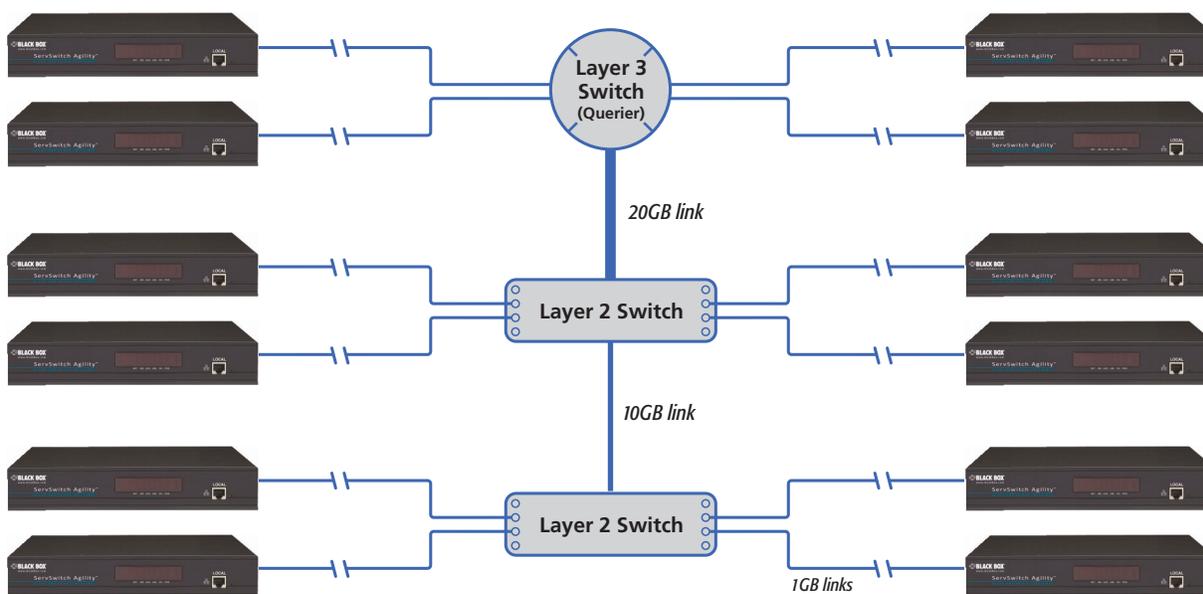
Figure A-1. Recommended layout for networking Agility local and remote units where IGMP snooping is used

Note: From firmware version 3.0, tree and hierarchical structures of network switches are also supported. The Transmitter now joins its own multicast group so there is always a route from the querier to the transmitter which was previously missing in firmware versions 2.9 and below.

- Use no more than two cascade levels.

- Ensure high bandwidth between the two L2 switches and very high bandwidth between the top L2 and the L3. Typically 10GB and 20GB, respectively for 48 port L2 switches.

A.4 Configuring the switches and devices

The layout is vital but so too is the configuration:

• Enable IGMP Snooping on all L2 switches.

• Ensure that IGMP Fast-Leave is enabled on all switches with Agility units connected directly to them.

• Enable the L3 switch as an IGMP Querier.

• Enable Spanning Tree Protocol (STP) on all switches and importantly also enable portfast (only) on all switch ports that have Agility units connected.

• If any hosts will use any video resolutions using 2048 horizontal pixels (e.g. 2048 x 1152), ensure that Jumbo Frames are enabled on all switches.

• Choose an appropriate forwarding mode on all switches. Use Cut-through if available, otherwise Store and forward.

• Optimize the settings on the Agility transmitters:

  • If moving video images are being shown frequently, then leave Frame Skipping at a low percentage and instead reduce the Peak bandwidth limiter.

  • Where screens are quite static, try increasing the Background Refresh interval and/or increasing the Frame skipping percentage setting.

  Make changes to the Agility transmitters one at a time, in small steps, and view typical video images so that you can attribute positive or negative results to the appropriate control.

• Ensure that all Agility units are fully updated to the latest firmware version (at least v3.3).

Appendix B. Troubleshooting

Problem: The video image of the Agility receiver shows horizontal lines across the screen.

This issue is known as *Blinding* because the resulting video image looks as though you're viewing it through a venetian blind.

When video is transmitted by Agility units, the various lines of each screen are divided up and transmitted as separate data packets. If the reception of those packets is disturbed, then blinding is caused. The lines are displayed in place of the missing video data packets.

There are several possible causes for the loss of data packets:

- Incorrect switch configuration. The problem could be caused by multicast flooding, which causes unnecessary network traffic. This is what IGMP snooping is designed to combat, however, there can be numerous causes of the flooding.

- Speed/memory bandwidth issues within one or more switches. The speed and capabilities of different switch models varies greatly. If a switch cannot maintain pace with the quantity of data being sent through it, then it will inevitably start dropping packets.

- One or more Agility units may be outputting Jumbo frames due to the video resolution (2048 horizontal pixels) being used. If jumbo frames are output by a Agility unit, but the network switches have not been configured to use jumbo frames, the switches will attempt to break the large packets down into standard packets. This process introduces a certain latency and could be a cause for dropped packets.

- One or more Agility units may be using an old firmware version. Firmware versions prior to v2.1 exhibited an issue with the timing of IGMP join and leave commands that caused multicast flooding in certain configurations.

Remedies:

- Ensure that IGMP snooping is enabled on all switches within the subnet.

- Where each Agility unit is connected as the sole device on a port connection to a switch, enable IGMP Fast-Leave (aka Immediate Leave) to reduce unnecessary processing on each switch.

- Check the video resolution(s) being fed into the Agility transmitters. If resolutions using 2048 horizontal pixels are unavoidable then ensure that Jumbo frames are enabled on all switches.

- Check the forwarding mode on the switches. If *Store and forward* is being used, try selecting *Cut-through* as this mode causes reduced latency on lesser switch designs.

- Ensure that one device within the subnet is correctly configured as an IGMP Querier, usually a layer 3 switch or multicast router.

- Ensure that the firmware in every Agility unit is version 3.3 or greater.

- Try adjusting the transmitter settings on each Agility to make the output data stream as efficient as possible.

Problem: The audio output of the Agility receiver sounds like a scratched record.

This issue is called Audio crackle and is a symptom of the same problem that produces blinding (see previous page). The issue is related to missing data packets.

Remedies:

As per blinding discussed above.

Problem: The mouse pointer of the Agility receiver is slow or sluggish when moved across the screen.

This issue is often related to either using dithering on the video output of one or more transmitting computers or using VGA-to-DVI video converters.

Dithering is used to improve the perceived quality and color depth of images by diffusing or altering the color of pixels between video frames. This practice is commonly used on Apple Mac computers using ATI or Nvidia graphics cards. VGA-to-DVI converters unwittingly produce a similar issue by creating high levels of pixel background noise.

Agility units attempt to considerably reduce network traffic by transmitting only the pixels that change between successive video frames. When dithering is enabled and/or VGA-to-DVI converters are used, this can have the effect of changing almost every pixel between each frame, thus forcing the Agility transmitter to send the whole of every frame: resulting in greatly increased network traffic and what's perceived as sluggish performance.

Remedies:

- Linux PCs

  Check the video settings on the PC. If the Dither video box option is enabled, disable it.

- Apple Mac with Nvidia graphics

  Use the Black Box utility for Mac's – Contact technical support.

- Apple Mac with ATI graphics

  Use the Agility Dual series unit with Magic Eye dither removal feature.

- Windows PCs

  If you suspect these issues with PC's, contact technical support for assistance.

- Replace old VGA adapters on host computers with DVI video cards.

Problem: iPATH Agility Controller cannot locate working Agility units.

There are a few possible causes:

- The Agility units must be reset back to their zero config IP addresses for iPATH Agility Controller discovery. If you have a working network of Agility unit's without iPATH Agility Controller and then add iPATH Agility Controller to the network, the iPath manager will not discover the Agility units until they are reset to the zero config IP addresses.

- This could be caused by Layer 2 Cisco switches that have Spanning Tree Protocol (STP) enabled but do not also have *portfast* enabled on the ports to which Agility units are connected. Without portfast enabled, Agility units will all be assigned the same zero config IP address at reboot and iPATH Agility Controller will only acquire them one at a time on a random basis.

  You can easily tell whether portfast is enabled on a switch that is running STP: When you plug the link cable from a working Agility unit into the switch port, check how long it takes for the port indicator to change from orange to green. If it takes roughly one second, portfast is on; if it takes roughly thirty seconds then portfast is disabled.

Remedies:

- Ensure that the Agility units and the iPATH Agility Controller manager are located within the same subnet. iPATH Agility Controller cannot cross subnet boundaries.

- Manually reset the Agility units to their zero config IP addresses.

- Enable portfast on all switch ports that have Agility units attached to them or try temporarily disabling STP on the switches while iPATH Agility Controller is attempting to locate Agility units.

Appendix C. Redundant servers: Setting up and swapping out

This appendix contains two main sections related to the creation and repair of iPATH Agility Controller installations that employ redundancy.

• Setting up iPATH Agility Controller redundancy - below

• Swapping out an iPATH Agility Controller - on next page

C.1 Setting up iPATH Agility Controller redundancy

This section details the steps required to successfully configure two iPATH units as primary and secondary servers.

1 Set the Rôle entry to **Primary** on the primary server.

2 Configure its Ethernet port 1 Address.

3 Ensure that password requirements is set to **NO**.

4 Add the new secondary iPATH Agility Controller to the network. The secondary server must have the same license as the primary. It is not possible to have two servers with different licenses in a cluster. This unit must have its factory default settings in place. The new server will appear within the main Servers tab and be identified as being Unconfigured.

5 Wait five minutes for automatic server replication to take place and the backup database to be transferred from the primary unit. After this period, the new secondary server will be added to the list on the main Servers tab. Its Rôle will be shown as backup and its Status as standby.

Note: If the transfer of the backup database is interrupted and only a partial database is transferred, then the problem will be reported within the management server page. If this occurs, it will not be possible to log in to the backup database and the firmware version of the backup will be reported as V. After five minutes, you should be given the options of Reboot and Factory Reset. Choose the Factory Reset option in order to clear this issue.

6 You can now configure the secondary server in either of two ways:

• Click the ✏ icon to configure the server remotely from the primary server.

• Click the 🔧 icon to open a restricted page in order to configure the server directly from its own IP address. If you use this option, the configuration options are limited to: view the logs; update/reset the iPATH Agility Controller and configure this server.

C.2 Operation of Redundancy

If the Primary server fails for any reason (for example, loss of power or a network issue) then the secondary server will failover. This will happen automatically without any user intervention, however it is not instantaneous. The failover time required is the value entered in the primary timeout plus 30 seconds for the process to happen. The Agility extenders will start communication with the second IP address that is stored in their configuration and the redundant server will take control of the Agility units. When the redundant server is acting as the primary it is not possible to add any new devices or change the configuration. If this is required then the backup server can be promoted to be the primary.

When the primary server comes back online then it will resume its role as the primary. If however the backup server has been promoted to primary, when the primary server comes back its role will need to be factory reset back to the backup. It is not possible to have two primary servers on the same network.

Both the primary and the backup server periodically synchronize their databases to ensure that they are identical. If for any reason the backup server is powered down then any changes to the system configuration will not be maintained by the backup server.

C.3 Swapping out an iPATH Agility Controller

Once Agility devices have been configured to run with an iPATH Agility Controller, their default IP addresses are automatically changed as part of the installation process. In this state the Agility devices become undetectable to any new iPATH Agility Controller that does not have access to the database of devices. Therefore, if an existing iPATH Agility Controller needs to be replaced within an installation, follow one of the basic procedures given here to smooth the transition.

The correct procedure to use depends on whether you are using a solo iPATH Agility Controller (firmware versions below 3.0 can only be used as solo servers) or a pair of iPATH Agility Controllers in a primary/backup redundancy arrangement:

C.3.1 For solo iPATH Agility Controllers

1 Before connecting the new iPATH Agility Controller to the main network, connect the new iPATH Agility Controller to a network switch that is isolated from the main network.

2 Use a computer connected to the same switch to login to the new iPATH Agility Controller management suite.

3 Set the Rôle entry to Solo.

4 Set the IP address of the new iPATH Agility Controller to match that of the original unit.

5 Restore a backup file of the original iPATH Agility Controller database to the new device.

6 Remove the original iPATH Agility Controller from the network. Connect the new iPATH Agility Controller in its place and power up.

7 All the devices will appear as offline. Using a paperclip, perform a factory reset on all the Agility endpoints so as they acquire the new certificate and keys. All Agility units require a minimum of firmware version 3.3.

C.3.2 For dual iPATH installations using redundancy

The correct procedure depends on which iPATH Agility Controller has failed:

Primary server failure

1 Promote the backup server to be the primary server.

2 Delete the failed server from the database.

3 Replace the faulty primary iPATH Agility Controller with a replacement unit that has the same license version and has its default factory settings in place.

4 The replacement server will begin communicating with the primary server and download the database so that it can operate as the backup server. This process may take ten minutes.

5 Reboot the Agility endpoints at the earliest opportunity.

Backup server failure

1 Delete the failed server from the database.

2 Replace the failed backup server with a new unit that has the same license version and has its default factory settings in place.

3 The replacement server will begin communicating with the primary server and download the database so that it can operate as the backup server. This process may take ten minutes.

4 Reboot the Agility endpoints at the earliest opportunity.

Warning: If step 4, rebooting the Agility endpoints, does not happen then the Agility endpoints will be offline if a failover occurs and will need to be factory reset with a paperclip.

C.3.3 Starting from scratch

If none of the above procedures are used, then the following will be necessary. This will require a certain amount of effort because each Agility unit must be visited and reset, plus the iPATH database will need to be fully reconfigured.

1 Place a new iPATH Agility Controller into the network and then perform a factory reset on every Agility device. This will force the Agility units back to their default states whereupon they will announce themselves to the new iPATH Agility Controller.

2 Use a computer connected to the same network to login to the new iPATH Agility Controller management suite and begin to recreate the database of devices and users.

Appendix D. Upgrade Licence

iPATH Agility Controllers are licenced according to the number of devices that can be managed. As your installation grows you can purchase an updated iPATH licence at any time using the following procedure. Four licences are available, ranging from a maximum of 24 managed devices up to a maximum of 288:

- iPATH-24-48UPG - increases the maximum number of managed devices from 24 to 48.
- iPATH-48-96UPG - increases the maximum number of managed devices from 48 to 96.
- iPATH-96-192UPG - increases the maximum number of managed devices from 96 to 192.
- iPATH-192-288UPG - increases the maximum number of managed devices from 192 to 288.

D.1 To upgrade your iPATH licence

1 Visit the Dashboard > Settings > General page of the iPATH unit to be upgraded. At the bottom of the page, click the 'upgrade licence' link:
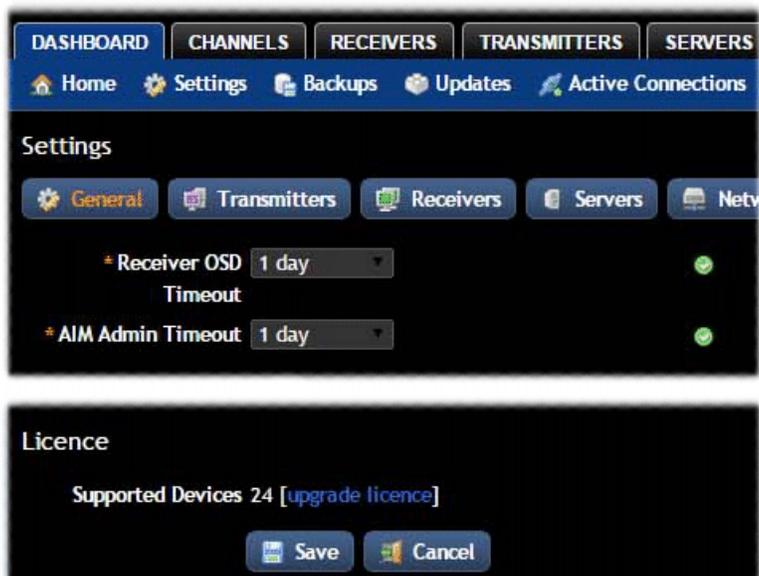
The subsequent file dialog will show a Product Code that is unique to your iPATH Agility Controller.

2 Contact your supplier and quote all of the following:

- The unique product code,
- The serial number of the iPATH Agility Controller (marked on a label on the base of the unit),
- The current number of supported devices, and
- The number of devices to which you wish to upgrade.

3 The supplier will provide a licence key, which is unique to unit to the unit to be upgraded. Enter the new licence key into the blank entry in the page shown above.

Note: It is important that you only enter the licence key into the specific iPATH unit.

If the upgrade is successful, the new number of supported devices will be shown in the Dashboard > Settings > General page.

Appendix E. Glossary

E.1 Internet Group Management Protocol

Where a Agility transmitter is required to stream video to two or more receivers, multicasting is the method used.

Multicasting involves the delivery of identical data to multiple receivers simultaneously without the need to maintain individual links. When multicast data packets enter a subnet, the natural reaction of the switches that bind all the hosts together within the subnet, is to spread the multicast data to all of their ports. This is referred to as Multicast flooding and means that the hosts (or at least their network interfaces) are required to process plenty of data that they didn't request. IGMP offers a partial solution.

The Internet Group Management Protocol (IGMP) is designed to prevent multicast flooding by allowing Layer 3 switches to check whether host computers within their care are interested in receiving particular multicast transmissions. They can then direct multicast data only to those points that require it and can shut off a multicast stream if the subnet has no recipients.

There are currently three IGMP versions: 1, 2 and 3, with each version building upon the capabilities of the previous one:

- IGMPv1 allows host computers to opt into a multicast transmission using a Join Group message, it is then incumbent on the router to discover when they no longer wish to receive; this is achieved by polling them (see IGMP Querier below) until they no longer respond.

- IGMPv2 includes the means for hosts to opt out as well as in, using a Leave Group message.

- IGMPv3 encompasses the abilities of versions 1 and 2 but also adds the ability for hosts to specify particular sources of multicast data.

Agility units make use of IGMPv2 when performing multicasts to ensure that no unnecessary congestion is caused.

E.1.2 IGMP Snooping

The IGMP messages are effective but only operate at layer 2 - intended for routers to determine whether multicast data should enter a subnet. A relatively recent development has taken place within the switches that glue together all of the hosts within each subnet: IGMP Snooping. IGMP snooping means these layer 2 devices now have the ability to take a peek at the IGMP messages. As a result, the switches can then determine exactly which of their own hosts have requested to receive a multicast – and only pass on multicast data to those hosts.

E.1.3 IGMP Querier

When IGMP is used, each subnet requires one Layer 3 switch to act as a Querier. In this lead role, the switch periodically sends out IGMP Query messages and in response all hosts report which multicast streams they wish to receive. The Querier device and all snooping Layer 2 switches, then update their lists accordingly (the lists are also updated when Join Group and Leave Group (IGMPv2) messages are received).

E.1.4 IGMP Fast-Leave (aka Immediate Leave)

When a device/host no longer wishes to receive a multicast transmission, it can issue an IGMP Leave Group message as mentioned above. This causes the switch to issue an IGMP Group-Specific Query message on the port (that the Leave Group was received on) to check no other receivers exist on that connection that wish to remain a part of the multicast. This process has a cost in terms of switch processor activity and time.

Where Agility units are connected directly to the switch (with no other devices on the same port) then enabling IGMP Fast-Leave mode means that switches can immediately remove receivers without going through a full checking procedure. Where multiple units are regularly joining and leaving multicasts, this can speed up performance considerably.

E.2 Jumbo frames (Jumbo packets)

Since its commercial introduction in 1980, the Ethernet standard has been successfully extended and adapted to keep pace with the ever improving capabilities of computer systems. The achievable data rates, for instance, have risen in ten-fold leaps from the original 10Mbit/s to a current maximum of 100Gbit/s.

While data speeds have increased massively, the standard defining the number of bytes (known as the Payload) placed into each data packet has remained resolutely stuck at its original level of 1500 bytes. This standard was set during the original speed era (10Mbits/s) and offered the best compromise at that speed between the time taken to process each packet and the time required to resend faulty packets due to transmission errors.

But now networks are much faster and files/data streams are much larger; so time for a change? Unfortunately, a wholesale change to the packet size is not straightforward as it is a fundamental standard and changing it would mean a loss of backward compatibility with older systems.

Larger payload options have been around for a while, however, they have often been vendor specific and at present they remain outside the official standard. There is, however, increased consensus on an optional 'Jumbo' payload size of 9000 bytes and this is fully supported by the Agility units.

Jumbo frames (or Jumbo packets) offer advantages for Agility units when transmitting certain high resolution video signals across a network. This is because the increased data in each packet reduces the number of packets that need to be transferred and dealt with - thus reducing latency times.

The main problem is that for jumbo frames to be possible on a network, all of the devices on the network must support them.

E.3 Spanning Tree Protocol (STP)

In order to build a robust network, it is necessary to include certain levels of redundancy within the interconnections between switches. This will help to ensure that a failure of one link does not lead to a complete failure of the whole network.

The danger of multiple links is that data packets, especially multicast packets, become involved in continual loops as neighbouring switches use the duplicated links to send and resend them to each other.

To prevent such bridging loops from occurring, the Spanning Tree Protocol (STP), operating at layer 2, is used within each switch. STP encourages all switches to communicate and learn about each other. It prevents bridging loops by blocking newly discovered links until it can discover the nature of the link: is it a new host or a new switch?

The problem with this is that the discovery process can take up to 50 seconds before the block is lifted, causing problematic timeouts.

The answer to this issue is to enable the portfast variable for all host links on a switch. This will cause any new connection to go immediately into forwarding mode. However, take particular care not to enable portfast on any switch to switch connections as this will result in bridging loops.

E.4 Forwarding modes

In essence, the job of a layer 2 switch is to transfer as fast as possible, data packets arriving at one port out to another port as determined by the destination address. This is known as data forwarding and most switches offer a choice of methods to achieve this. Choosing the most appropriate forwarding method can often have a sizeable impact on the overall speed of switching:

• **Store and forward** is the original method and requires the switch to save each entire data packet to buffer memory, run an error check and then forward if no error is found (or otherwise discard it).

• **Cut-through** was developed to address the latency issues suffered by some store and forward switches. The switch begins interpreting each data packet as it arrives. Once the initial addressing information has been read, the switch immediately begins forwarding the data packet while the remainder is still arriving. Once all of the packet has been received, an error check is performed and, if necessary, the packet is tagged as being in error. This checking 'on-the-fly' means that cut-through switches cannot discard faulty packets themselves. However, on receipt of the marked packet, a host will carry out the discard process.

• **Fragment-free** is a hybrid of the above two methods. It waits until the first 64 bits have been received before beginning to forward each data packet. This way the switch is more likely to locate and discard faulty packets that are fragmented due to collisions with other data packets.

• **Adaptive** switches automatically choose between the above methods. Usually they start out as a cut-through switches and change to store and forward or fragment-free methods if large number of errors or collisions are detected.

So which one to choose? The *Cut-through* method has the least latency so is usually the best to use with Agility units. However, if the network components and/or cabling generate a lot of errors, the *Store and forward* method should probably be used. On higher end store and forward switches, latency is rarely an issue.

E.5 Layer 2 and Layer 3: The OSI model

When discussing network switches, the terms Layer 2 and Layer 3 are very often used. These refer to parts of the Open System Interconnection (OSI) model, a standardized way to categorize the necessary functions of any standard network.

There are seven layers in the OSI model (see Figure C-1) and these define the steps needed to get the data created by you (imagine that you are Layer 8) reliably down onto the transmission medium (the cable, optical fiber, radio wave, etc.) that carries the data to another user; to complete the picture, consider the transmission medium is Layer 0. In general, think of the functions carried out by the layers at the top as being complex, becoming less complex as you go lower down.

LAYER 7	Application		LAYER 7
LAYER 6	Presentation		LAYER 6
LAYER 5	Session		LAYER 5
LAYER 4	Transport		LAYER 4
LAYER 3	Network		LAYER 3
LAYER 2	Data Link		LAYER 2
LAYER 1	Physical		LAYER 1

Network connection

Figure C-1. A representation of the seven layers defined by the OSI Model

As your data travel down from you towards the transmission medium (the cable), they are successively encapsulated at each layer within a new wrapper (along with a few instructions), ready for transport. Once transmission has been made to the intended destination, the reverse occurs: Each wrapper is stripped away and the instructions examined until finally only the original data are left.

So why are Layer 2 and Layer 3 of particular importance when discussing Agility? Because the successful transmission of data relies upon fast and reliable passage through network switches – and most of these operate at either Layer 2 or Layer 3.

The job of any network switch is to receive each incoming network packet, strip away only the first few wrappers to discover the intended destination then rewrap the packet and send it in the correct direction.

In simplified terms, the wrapper that is added at Layer 2 (by the sending system) includes the physical address of the intended recipient system, i.e. the unique MAC address (for example, 09:f8:33:d7:66:12) that is assigned to every networking device at manufacture. Deciphering recipients at this level is more straightforward than at Layer 3, where the address of the recipient is represented by a logical IP address (e.g. 192.168.0.10) and requires greater knowledge of the surrounding network structure. Due to their more complex circuitry, Layer 3 switches are more expensive than Layer 2 switches of a similar build quality and are used more sparingly within installations.

Appendix F - iPATH API

The iPATH API provides access for external applications to key routines used within the iPATH Agility Controller. This appendix provides a reference to the available methods.

API version: 4

Changelog

•v4 (iPATH v4.1) - added create_channel, delete_channel; updated get_channels.

•v3 (iPATH v3.2) - added create_preset, delete_preset.

•v2 (iPATH v2.3) - added get_devices, get_channels, connect_channel, disconnect_channel. Updated version compatibility information.

•v1 (iPATH v1.3) - added login, logout, get_presets, connect_preset, disconnect_preset

Methods

login

logout

get_devices

get_channels

get_presets

connect_channel

connect_preset

disconnect_channel

disconnect_preset

create_preset

delete_preset

create_channel

delete_channel

login

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

The API will require a valid iPATH user's login credentials to be presented in the first request. The API will return an authentication code, which must be passed in all future requests. This authentication code can be re-used until a logout request is made, at which point the authentication code will no longer be valid.

The concept of an 'anonymous user' can apply to the API. If no login username and password are provided, the API will return an authentication token for the anonymous user (either the same one as for the OSD, or else an 'anonymous API user' account can be created).

Input parameters:
- username

- password

- v (the iPATH API version this request is designed for)

Output values:
- timestamp - the current server time

- version - the current API version number

- token - an authentication code for future API requests

- success

Examples

Input:
/api/?v=1&method=login&username=xxxxx&password=xxxxx

Output:
<api_response>

  <version>1</version>

  <timestamp>2012-12-14 12:12:12</timestamp>

  <success>1</success>

  <token>5cf494a71c29e9465a57a81e0a2d602c</token>

</api_response>

or

<api_response>

  <version>1</version>

  <timestamp>2012-12-14 12:12:12</timestamp>

  <success>0</success>

  <errors>

    <error>

      <code>2</code>

      <msg>Invalid username or password</msg>

    </error>

  </errors>

</api_response>

877-877-2269 l blackbox.com

logout

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards

The authentication token provided by the Login function can be used until the logout function is called.

Input parameters:
- token

- v (the iPATH API version this request is designed for)

Output values:
- timestamp - the current server time

- success - 0 = fail, 1 = success

Examples

Input:
/api/?method=logout&token=xxxxx&v=1

Output:
<api_response>

   <version>1</version>

   <timestamp>2011-02-04 15:24:15</time>

   <success>1</success>

</api_response>

or

<api_response>

   <version>1</version>

   <timestamp>2012-12-12 12:12:12</timestamp>

   <success>0</success>

   <errors>

     <error>

       <code>3</code>

       <msg>Error logging out (you may already have logged out)</msg>

     </error>

   </errors>

</api_response>

get_devices

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards

This function returns a list of devices.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- device_type ('rx' = receivers, 'tx' = transmitters. Default = 'rx')

- filter_d_name (Optional. Device name search string)

- filter_d_description (Optional. Device description search string)

- filter_d_location (Optional. Device location search string)

- sort (Optional. Sort results by 'name'/'description'/'location'. Default = 'name')

- sort_dir (Optional. Sort direction for results 'asc'/'desc'. Default = 'asc')

- status (Optional. '','outdated_aim_ip','rebooting','offline','outdated_firmware','invalid_backup_firmware','rebooting','upgrading_firmware','backup_mode')

- show_all (Optional. If set and not blank, shows all receivers, not just those the logged-in user is permitted to use)

- page (page number to start showing results for, default = 1)

- results_per_page (number of results per page, default = 1000)

Output values:

- version - the current API version number

- timestamp - the current server time

- success

- page (page number)

- results_per_page (number of results per page, default = unlimited)

- total_devices - the total number of devices

- count_devices - the number of devices on this page

get_devices (continued)

- for each device:

- attribute: item (e.g. 17th device)

- d_id (device ID)

- d_mac_address (MAC address for interface 1)

- d_mac_address2 (MAC address for interface 2)

- d_name (device name)

- d_online (0 = interface 1 offline, 1 = interface 1 online)

- d_online2 (0 = interface 2 offline, 1 = interface 2 online)

- d_type (rx, tx)

- d_version (1 = ACR1000A-R/ACR1000A-T, 2 = all other devices)

- d_variant ('b' = ACR1002A-T, 'v' = ACR1012A-T, 's' = ACR1000A-R-R2/ACR1000A-T-R2, 't' = ACR1020A-R/ACR1020A-T)

- d_ip_address (IP address for interface 1)

- d_ip_address2 (IP address for interface 2)

- d_description (device description)

- d_location (device location)

- d_configured (0 = no, 1 = yes)

- d_valid_firmware (0 = no, 1 = yes)

- d_valid_backup_firmware (0 = no, 1 = yes)

- d_firmware (firmware version, e.g. 2.5.17879)

- d_backup_firmware (backup firmware version)

- d_date_added (Date device added to iPATH network e.g. 2012-07-13 22:17:22)

- d_status (0 = device offline, 1 = device online, 2 = rebooting, 4 = firmware_upgrading, 6 = running backup firmware)

The following property is only returned for transmitters:

- count_transmitter_channels (the number of channels containing this transmitter)

The following properties are only returned for receivers:

- con_exclusive (0/1 - if the last connection is/was in private mode)

- con_control (1/2/3 - 1 if the last connection is/was video-only, 2 if in exclusive mode, 3 if in shared mode)

- con_start_time (start time of last connection e.g. 2012-09-07 13:33:17)

- con_end_time (empty if connection still active, else date/time the connection was ended e.g. 2012-09-07 13:33:17)

- u_username (username of the user who initiated the last connection)

- u_id (user ID of the user who initiated the last connection)

- c_name (name of the channel last connected)

- count_receiver_groups (the number of receiver groups this receiver is a part of)

- count_receiver_presets (the number of presets this receiver is a part of)

- count_users (the number of users who have access to this receiver)

Examples

Input:
/api/?v=2&method=get_devices&token=xxxxx

/api/?v=2&method=get_devices&device_type=tx&page=2&results_per_page=3&token=xxxxx

Output:

```
<api_response>
  <version>2</version>
  <timestamp>2012-09-12 14:56:11</timestamp>
  <success>1</success>
  <page>2</page>
  <results_per_page>3</results_per_page>
  <total_devices>12</total_devices>
  <count_devices>3</count_devices>
  <devices>
    <device item="4">
      <d_id>170</d_id>
      <d_mac_address>00:0F:58:01:6E:3D</d_mac_address>
      <d_mac_address2>00:0F:58:5B:6E:3D</d_mac_address2>
      <d_name>RX 123</d_name>
      <d_online>1</d_online>
      <d_online2>0</d_online2>
      <d_type>rx</d_type>
      <d_version>2</d_version>
      <d_variant></d_variant>
      <d_ip_address>10.10.10.66</d_ip_address>
      <d_ip_address2>10.10.10.67</d_ip_address2>
      <d_description></d_description>
      <d_location>Server Rack 3</d_location>
      <d_configured>1</d_configured>
      <d_valid_firmware>1</d_valid_firmware>
      <d_valid_backup_firmware>1</d_valid_backup_firmware>
      <d_firmware>2.3.16682</d_firmware>
      <d_backup_firmware>2.3.16682</d_backup_firmware>
      <d_date_added>2012-07-14 01:37:07</d_date_added>
      <d_status>1</d_status>
```

877-877-2269 | blackbox.com

```
        <con_exclusive>0</con_exclusive>

        <con_control>1</con_control>

        <con_start_time>2012-09-07 13:33:19</con_start_time>

        <con_end_time/>

        <u_username>admin</u_username>

        <u_id>1</u_id>

        <c_name>Channel 1</c_name>

        <count_receiver_groups>1</count_receiver_groups>

        <count_receiver_presets>2</count_receiver_presets>

        <count_users>1</count_users>

      </device>

   </devices>

</api_response>

<api_response>

   <version>2</version>

   <timestamp>2012-09-12 14:56:11</timestamp>

   <success>1</success>

   <page>1</page>

   <results_per_page>1</results_per_page>

   <total_devices>1</total_devices>

   <count_devices>1</count_devices>

   <devices>

      <device item="1">

        <d_id>64</d_id>

        <d_mac_address>00:0F:58:01:56:85</d_mac_address>

        <d_mac_address2>00:0F:58:5B:56:85</d_mac_address2>

        <d_name>TX 456</d_name>

        <d_online>0</d_online>

        <d_online2>0</d_online2>

        <d_type>tx</d_type>

        <d_version>1</d_version>

        <d_variant></d_variant>

        <d_ip_address>1.1.201.31</d_ip_address>

        <d_ip_address2>1.1.201.32</d_ip_address2>

        <d_description></d_description>

        <d_location></d_location>

        <d_configured>1</d_configured>

        <d_valid_firmware>1</d_valid_firmware>
```

```
        <d_valid_backup_firmware>1</d_valid_backup_firmware>

        <d_firmware>2.1.15747</d_firmware>

        <d_backup_firmware>2.1.15747</d_backup_firmware>

        <d_date_added>2012-07-13 17:50:04</d_date_added>

        <d_status>0</d_status>

        <count_transmitter_channels>3</count_transmitter_channels>

    </device>

  </devices>

</api_response>
```

get_channels

This method was last updated in API version 4, and is compatible with API requests from version 2 onwards.

This function returns a list of channels available to the authenticated user, for a specific receiver. It was updated in version 4 to include additional information.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- page (page number to start showing results for, default = 1)

- results_per_page (number of results per page, default = 1000)

- device_id (ID of the receiver that this channel will be connected to. Recommended to ensure full checks for connection mode availability.

- filter_c_name (channel name search string)

- filter_c_description (channel description search string)

- filter_c_location (channel location search string)

- filter_favourites (set this non-empty to only show a user's favourites)

Output values:

- version - the current API version number

- timestamp - the current server time

- success

- page (page number)

- results_per_page (number of results per page, default = unlimited)

- count_channels - the number of channels on this page, available to the authenticated user

get_channels (continued)

- for each channel:

   - attribute: item (e.g. 17th channel)

   - c_id (channel id)

         - c_name (channel name)

         - c_description (channel description)

         - c_location (channel location)

         - c_favourite (true if this channel is in the user's favourites, 0-9 if it's a numbered shortcut)

   - view_button (disabled/enabled/hidden - whether the user can connect to the preset in video-only mode. disabled = no, because something is in use by someone else. hidden = never. enabled = yes

      If the device_id of the proposed receiver to be used in the connection is not provided, this will not necessarily be an accurate indication of whether other connections may actually interfere)

   - shared_button (disabled/enabled/hidden - as above, but in shared mode)

   - control_button (disabled/enabled/hidden - as above, but in exclusive mode)

   - exclusive_button (disabled/enabled/hidden - as above, but in private mode)

Additional channel output values in version 4:

   - c_video1 (device ID)

   - c_video1_head (1l2)

   - c_video2 (device ID)

   - c_video2_head (1l2)

   - c_audio (device ID)

   - c_usb (device ID)

   - c_serial (device ID)

Examples

Input:
/api/?v=2&method=get_channels&token=xxxxx

Version 2 output:
<api_response>

   <version>2</version>

   <timestamp>2012-12-14 12:12:12</timestamp>

   <success>1</success>

   <page>1</page>

   <results_per_page>10</results_per_page>

   <count_channels>2</count_channels>

   <channel item="1">

      <c_id>3</c_id>

```
            <c_name>Channel 1</c_name>

            <c_description>Description for Channel 1</c_description>

            <c_location>Location of Channel 1</c_location>

            <c_favourite>false</c_favourite>

            <view_button>disabled</view_button>

            <shared_button>disabled</shared_button>

            <control_button>disabled</control_button>

            <exclusive_button>disabled</exclusive_button>

        </channel>

        <channel item="2">

            <c_id>5</c_id>

            <c_name>Channel 2</c_name>

            <c_description>Description for Channel 2</c_description>

            <c_location>Location of Channel 2</c_location>

            <c_favourite>2</c_favourite>

            <view_button>enabled</view_button>

            <shared_button>enabled</shared_button>

            <control_button>enabled</control_button>

            <exclusive_button>hidden</exclusive_button>

        </channel>

</api_response>
```

877-877-2269 | blackbox.com

get_presets

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards.

This simple function returns a list of presets available to the authenticated user.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- results_per_page (number of results per page, default = 1000)

- page (page number to start showing results for, default = 1)

Output values:

- version - the current API version number

- timestamp - the current server time

- success

- page (page number)

- results_per_page (number of results per page, default = unlimited)

- total_presets - the total number of presets available to the authenticated user

- count_presets - the number of presets on this page, available to the authenticated user

- for each connection_preset:

  - attribute: item (e.g. 17th preset)

  - cp_id (preset id)

        - cp_name (preset name)

        - cp_description (preset description)

        - cp_pairs (the number of channel-receiver pairs in this preset)

  - problem_cp_pairs (the number of channel-receiver pairs that are mis-configured

    (e.g. receiver offline, receiver not defined)

  - cp_active (whether all, any, or none of the channel-receiver pairs in this preset are

    currently connected; values are 'full', 'partial', and 'none')

  - connected_rx_count (the number of receivers in this preset that are already connected)

  - view_button (disabled/enabled/hidden - whether the user can connect to the preset in video-only mode.

    disabled = no, because something is in use by someone else.
        hidden = never. enabled = yes)

  - shared_button (disabled/enabled/hidden - as above, but in shared mode)

  - control_button (disabled/enabled/hidden - as above, but in exclusive mode)

  - exclusive_button (disabled/enabled/hidden - as above, but in private mode)

Examples

Input:
/api/?v=1&method=get_presets&token=xxxxx

Output:
```
<api_response>
  <version>1</version>
  <timestamp>2012-12-14 12:12:12</timestamp>
  <success>1</success>
  <page>1</page>
  <results_per_page>10</results_per_page>
  <total_presets>2</total_presets>
  <count_presets>2</count_presets>
  <connection_preset item="1">
    <cp_id>3</cp_id>
    <cp_name>Preset 1</cp_name>
    <cp_description>Description for Preset 1</cp_description>
    <cp_pairs>1</cp_pairs>
    <problem_cp_pairs/>
    <cp_active>full</cp_active>
    <connected_rx_count>1</connected_rx_count>
    <view_button>disabled</view_button>
    <shared_button>disabled</shared_button>
    <control_button>disabled</control_button>
    <exclusive_button>disabled</exclusive_button>
  </connection_preset>
  <connection_preset item="2">
    <cp_id>4</cp_id>
    <cp_name>Preset 2</cp_name>
    <cp_description>Description for Preset 2</cp_description>
    <cp_pairs>2</cp_pairs>
    <problem_cp_pairs/>
    <cp_active>none</cp_active>
    <connected_rx_count/>
    <view_button>enabled</view_button>
    <shared_button>hidden</shared_button>
    <control_button>hidden</control_button>
    <exclusive_button>hidden</exclusive_button>
  </connection_preset>
</api_response>
```

connect_channel

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards.

This simple function connects a receiver to a channel.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- c_id - the ID of the channel (acquired from get_channels)

- rx_id - the ID of the receiver (acquired from get_receivers)

- view_only (optional, 0/1 - defaults to 0)

- exclusive (optional, 0/1 - defaults to 0)

Output values:

- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (optional, if anything went wrong with connecting the channel)

Examples

Input:
/api/?v=2&method=connect_channel&token=xxxxx&c_id=1&rx_id=2&exclusive=1

Output:
```
<api_response>
   <version>2</version>
   <timestamp>2012-12-12 12:12:12</timestamp>
   <success>1</success>
</api_response>
```
or
```
<api_response>
   <version>2</version>
   <timestamp>2012-12-12 12:12:12</timestamp>
   <success>0</success>
   <errors>
     <error>
       <code>231</code>
       <msg>ERROR - private connection not available</msg>
     </error>
   </errors>
</api_response>
```

connect_preset

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards.

This simple function connects all channel-receiver pairs in a preset.

Input parameters:
- token

- v (the iPATH API version this request is designed for)

- id - the ID of the preset (acquired from get_presets)

- view_only (optional, 0/1 - defaults to 0)

- exclusive (optional, 0/1 - defaults to 0)

- force (optional, 0/1 - defaults to 0) - whether to ignore errors with some of the preset's pairs or not

Output values:
- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (optional, if anything went wrong with connecting the presets)

Examples

Input:
/api/?v=1&method=connect_preset&token=xxxxx&id=1&force=1

Output:
```
<api_response>
   <version>1</version>
   <timestamp>2012-12-12 12:12:12</timestamp>
   <success>1</success>
</api_response>
or
<api_response>
   <version>1</version>
   <timestamp>2012-12-12 12:12:12</timestamp>
   <success>0</success>
   <errors>
     <error>
       <code>210</code>
       <msg>".$config['error_codes'][210]."</msg>
     </error>
   </errors>
</api_response>
```

877-877-2269 l blackbox.com

disconnect_channel

This method was last updated in API version 2, and is compatible with API requests from version 2 onwards.

This function disconnects a receiver, a number of receivers, or all connected receivers.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- rx_id (ID(s) of the receiver, as an integer, or comma-separated set of integers.
        Optional. If not supplied, all connections will be ended)

- force - whether to disconnect existing connections by other users, or for offline   receivers

Output values:

- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

Examples

Input:

/api/?v=2&method=disconnect_channel&token=xxxxx (disconnect all your online, connected channels)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1 (disconnect channel 1, if you connected it and it's online)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,2,3 (disconnect channels 1, 2, and 3, if you connected them and they're online)

/api/?v=2&method=disconnect_channel&token=xxxxx&force=1 (force disconnect all connected channels)

/api/?v=2&method=disconnect_channel&token=xxxxx&rx_id=1,3&force=1 (force disconnect channels 1 and 3)

Output:

<api_response>

  <version>2</version>

  <timestamp>2012-12-12 12:12:12</timestamp>

  <success>1</success>

</api_response>

disconnect_preset

This method was last updated in API version 1, and is compatible with API requests from version 1 onwards.

This function disconnects all channel-receiver pairs in a preset, or disconnects ALL connections in the whole iPATH network.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- id (optional. If not supplied, all connections will be ended)

- force - whether to ignore errors with some of the preset's pairs or not

Output values:

- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=1&method=disconnect_preset&token=xxxxx&id=1&force=1

Output:
<api_response>

   <version>1</version>

   <timestamp>2012-12-12 12:12:12</timestamp>

   <success>1</success>

</api_response>

877-877-2269 l blackbox.com

create_preset

This method was last updated in API version 3, and is compatible with API requests from version 3 onwards

This function creates a new preset. The API user must have admin privileges to call this method successfully.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- name (the display name for the new preset)

- pairs (a comma-separated list of the channel ID–receiver ID pairs for the preset, where each ID in the pair is separated by a hyphen)

- allowed (the permitted connection modes for the preset. Optional; if omitted, the global setting will be inherited. Permitted values are:

    v   - video-only

    vs - video-only and shared

    s   - shared only

    e   - private only

    vse - any mode allowed)

Output values:

- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

- id (the ID of the new preset, if it was created)

Examples

Input:
/api/?v=3&method=create_preset&token=xxxxx&name=my_preset&pairs=1-1,1-2,2-3,2-4&allowed=vs

Output:
<api_response>

   <version>3</version>

   <timestamp>2012-12-12 12:12:12</timestamp>

   <success>1</success>

   <id>5</success>

</api_response>

delete_preset

This method was last updated in API version 3, and is compatible with API requests from version 3 onwards

This function deletes a preset. The API user must have admin privileges to call this method successfully.

Input parameters:
- token

- v (the iPATH API version this request is designed for)

- id (the ID of the preset to be deleted)

Output values:
- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=3&method=delete_preset&token=xxxxx&id=5

Output:
<api_response>

   <version>3</version>

   <timestamp>2012-12-12 12:12:12</timestamp>

   <success>1</success>

</api_response>

create_channel

This method was last updated in API version 4, and is compatible with API requests from version 4 onwards. This function creates a new channel. The API user must have admin privileges to call this method successfully. Note that, although the source device ID inputs are each optional, at least one is required.

Input parameters:

- token

- v (the iPATH API version this request is designed for)

- name (the display name for the new channel)

- desc (the display description for the new channel. Optional, default is empty.)

- loc (the display location for the new channel. Optional, default is empty.)

- allowed (the permitted connection modes for the channel. Optional; if omitted, the global setting will be inherited. Permitted values are:

    v   - video-only

    vs - video-only and shared

    s   - shared only

    e   - private only

    vse - any mode allowed)

- video1 (device ID of video source 1. Optional, default is empty.)

- video1head (video head number for source 1. Optional, default is 1.)

- video2 (device ID of video source 2. Optional, default is empty.)

- video2head (video head number for source 2. Optional, default is 1.)

- audio (device ID of the audio source. Optional, default is empty.)

- usb (device ID of the usb source. Optional, default is empty.)

- serial (device ID of the serial source. Optional, default is empty.)

- groupname (the name of a channel group of which the created channel will be a member. Optional, default is empty.)

Output values:

- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

- id (the ID of the new channel, if it was created)

Examples

Input:

/api/?v=4&method=create_channel&token=xxxxx&name=my_channel&video1=21&audio=81&groupname=my_channel_group

Output:

```
<api_response>
   <version>3</version>
   <timestamp>2012-12-12 12:12:12</timestamp>
   <success>1</success>
   <id>91</success>
</api_response>
```

delete_channel

This method was last updated in API version 4, and is compatible with API requests from version 4 onwards.

This function deletes a channel. The API user must have admin privileges to call this method successfully.

Input parameters:
- token

- v (the iPATH API version this request is designed for)

- id (the ID of the channel to be deleted)

Output values:
- version - the current API version number

- timestamp - the current server time

- success (0 = fail, 1 = success)

- errors (if anything failed, details are returned here)

Examples

Input:
/api/?v=4&method=delete_channel&token=xxxxx&id=5

Output:
<api_response>

   <version>4</version>

   <timestamp>2012-12-12 12:12:12</timestamp>

   <success>1</success>

</api_response>

About Black Box

Black Box Network Services is your source for an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 60 seconds or less.

ACR1000A-CTL, rev. 4.4 (RC2)