SNMP Management Module

USER MANUAL

B+B SMARTWORX

Powered by ADVANTECH

Advantech B+B SmartWorx - Americas
707 Dayton Road
Ottawa, IL 61350 USA
Phone (815) 433-5100
Fax (815) 433-5105

Advantech B+B SmartWorx - European Headquarters
Westlink Commercial Park
Oranmore, Co. Galway, Ireland
Phone +353 91-792444
Fax +353 91-792445

www.advantech-bb.com
support@advantech-bb.com

CONTENTS

LIST OF FIGURES

LIST OF TABLES

RADIO FREQUENCY INTERFERENCE STATEMENT

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

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits. This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

WARRANTY

Limited Lifetime Warranty

Effective for products of B+B SmartWorx shipped on or after May 1, 2013, B+B SmartWorx warrants that each such product shall be free from defects in material and workmanship for its lifetime. This limited lifetime warranty is applicable solely to the original user and is not transferable.

This warranty is expressly conditioned upon proper storage, installation, connection, operation and maintenance of products in accordance with their written specifications.

Pursuant to the warranty, within the warranty period, B+B SmartWorx, at its option will:

1. Replace the product with a functional equivalent;

2. Repair the product; or

3. Provide a partial refund of purchase price based on a depreciated value.

Products of other manufacturers sold by B+B SmartWorx are not subject to any warranty or indemnity offered by B+B SmartWorx, but may be subject to the warranties of the other manufacturers.

Notwithstanding the foregoing, under no circumstances shall B+B SmartWorx have any warranty obligations or any other liability for: (i) any defects resulting from wear and tear, accident, improper use by the buyer or use by any third party except in accordance with the written instructions or advice of the B+B SmartWorx or the manufacturer of the products, including without limitation surge and overvoltage conditions that exceed specified ratings, (ii) any products which have been adjusted, modified or repaired by any party other than B+B SmartWorx or (iii) any descriptions, illustrations, figures as to performance, drawings and particulars of weights and dimensions contained in the B+B SmartWorx' catalogs, price lists, marketing materials or elsewhere since they are merely intended to represent a general idea of the products and do not form part of this price quote and do not constitute a warranty of any kind, whether express or implied, as to any of the B+B SmartWorx' products

THE REPAIR OR REPLACEMENT OF THE DEFECTIVE ITEMS IN ACCORDANCE WITH THE EXPRESS WARRANTY SET FORTH ABOVE IS B+B SMARTWORX' SOLE OBLIGATION UNDER THIS WARRANTY. THE WARRANTY CONTAINED IN THIS SECTION SHALL EXTEND TO THE ORIGINAL USER ONLY, IS IN LIEU OF ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, AND ALL SUCH WARRANTIES AND INDEMNITIES ARE EXPRESSLY DISCLAIMED, INCLUDING WITHOUT LIMITATION (I) THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE AND OF MERCHANTABILITY AND (II) ANY WARRANTY THAT THE PRODUCTS ARE DO NOT INFRINGE OR VIOLATE THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY. IN NO EVENT SHALL B+B SMARTWORX BE LIABLE FOR LOSS OF BUSINESS, LOSS OF USE OR OF DATA INTERRUPTION OF BUSINESS, LOST PROFITS OR GOODWILL OR OTHER SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES. B&B ELECTRONIC SHALL DISREGARD AND NOT BE BOUND BY ANY REPRESENTATIONS, WARRANTIES OR INDEMNITIES MADE BY ANY OTHER PERSON, INCLUDING WITHOUT LIMITATION EMPLOYEES, DISTRIBUTORS, RESELLERS OR DEALERS OF B+B SMARTWORX WHICH ARE INCONSISTENT WITH THE WARRANTY, SET FORTH ABOVE.

ABOUT THE SNMP MANAGEMENT MODULE

The SNMP Management Module includes two twisted pair ports, one for management and one reserved for future use. The Management Module also features a DB-9 serial port. Both twisted pair ports include the AutoCross feature that automatically selects between a crossover workstation or straight-through, depending on the connected device.

An iMediaChassis series with an installed Management Module connects to the LAN via an external 10/100 twisted pair connection. Connect the chassis to the network by plugging one end of a CAT-5 twisted pair cable into the port labeled MGMT on the Management Module. Plug the other end of the cable into a device (e.g., switch, etc.) in the existing Ethernet network

HARDWARE INSTALLATION

In order to manage an iMediaChassis series, available in 20, 6, or 3 slots, install the SNMP Management Module. Slide the SNMP Management Module into the first slot, on the far left of the chassis, using the card guides, and secure the module to the chassis by tightening the captive screw. This slot is ONLY for the Management Module; do not install Application Modules such as media conversion and mode conversion modules in this slot.

SNMP MANAGEMENT MODULE LEDS

Each SNMP Management Module features several LEDs. The LED functions are:

LNK/ACT Glows green when a link is established on port. Glows green when data activity occurs.

FDX/COL Blinks amber when port is in Full-Duplex mode. Blinks amber when collisions occur; extinguished when port is operating in Half-Duplex mode.

TEMP Glows yellow when temperature of unit surpasses a user-defined Level, configurable through iView².

PS

FAN A / FAN B Glows amber when one power supply malfunctions.

Refer to specific iMediaChassis series manuals for details

CONFIGURING THE SNMP MODULE

Once connected to a network, assign the SNMP Management Module IP configuration information (e.g., IP address, subnet mask, etc.). There are four ways to do this:

- Using iConfig (Desktop version)
- Using the Webwerver version
- Using the Management Module's serial port
- Using DHCP (Dynamic Host Control Protocol); DHCP must be enabled through serial configuration or Telnet, via iConfig
- Telnet (Default IP=10.10.10.10; subnet mask 255.0.0.0)

In addition to assigning an IP address and subnet mask, the SNMP Management Module allows creation of community strings, assigning access rights, configuration of traps and more. iConfig offers more options than configuration via the serial port or Telnet. After assigning an IP address, use iView² or another SNMP compatible Network Management System (NMS) to remotely configure, monitor and manage the modules installed.

NOTE: iConfig is not available when using the Webserver version

	IView2	Serial	Telnet	iConfig
VLANS		ü	ü	
Modes		ü	ü	
IP	ü	ü	ü	ü
Subnet Mask	ü	ü	ü	ü
Default Gateway	ü	ü	ü	ü
Bandwidth	ü	ü	ü	
Software Updates	ü	ü TFTP	ü TFTP	ü

Table 1: Configuration Options iView² Desktop Version

SNMP WRITE LOCK (IMEDIACHASSIS SERIES)

There is an SNMP Write Lock switch on the iMediaChassis series; check the specific iMediaChassis manual for the location. The SNMP Write Lock switch prevents a new Management Module from re-configuring an iMcV-application module's settings (e.g. the status of features such as LinkLoss, FiberAlert, Force mode, etc.) made via SNMP on any previous management board(s).

NOTE
Leave this switch in the **NORMAL** position during day-to-day operation; the **LOCKED** position should only be used when changing the SNMP Management Module.

As stated, SNMP Management Modules can be removed and replaced as necessary. A saved PROM file can be downloaded to the second SNMP module to retain configuration settings.

Make sure the SNMP Write Lock switch is set to the **LOCKED** position. The PROM file should be saved periodically in case there is a need to replace the SNMP Management Module.

Saving the existing PROM creates a back-up file which can be used in the event that a unit or PROM update fails. It is recommended that the PROM be saved after the user is satisfied with his current configuration settings, as saving the PROM at this point will allow them to recover their configurations as well.

1. Open a session in iConfig to administer a device.
2. Choose the Administration tab.
3. Click the **Save PROM File** button.
4. The *Save as PROM* dialog box appears.

5. Choose a folder and then select the filename to be saved.
6. Click the **Save** button to save, the file is saved.
7. Add entries to the Notes box, if desired; then click **OK**. Click **Close** if notes are required.
8. Click **OK** to close Succeeded dialog box. (Prom Save was successful.)

NOTE
.BIN is the default extension.

If the Management Module is removed with the SNMP Write Lock switch set to NORMAL, all module revert to their hardware settings by default; for any module with on-board logic, refer to its manual for details. Hardware settings should be configured to match those made via SNMP. Always reconfigure application modules when moving them from one chassis' slot to another.

USING THE SNMP WRITE LOCK SWITCH

1. Ensure the SNMP Write Lock switch is set to **NORMAL**.
2. After configuring all application module settings via SNMP, use the iConfig application to make a backup copy of the SNMP management board's firmware.
3. If the SNMP Management Module needs to be replaced, set the SNMP Write Lock switch to **LOCKED**.
4. Remove the old SNMP module and replace with another SNMP module.
5. Connect to this SNMP module via iView² and then launch iConfig. Select the Administration tab and click on List Tasks. Highlight **Flashsav** and then click on the **Terminate** button.
6. Update the new board with the firmware backup made in Step 2.
7. Reboot the SNMP Management Module with the **Reboot** command to enable changes.
8. After rebooting, set the SNMP Write Lock switch back to **NORMAL**. The previously made settings to the application modules will be active.

NOTE
When removing an SNMP card with the SNMP Write Lock enabled (set to LOCKED), current application modules settings will not be changed. Never power-cycle the chassis while the SNMP Write Lock is enabled (except during Step 5 in the preceding process). This will revert the SNMP card back to its original factory settings. (iView² should only be accessed with the SNMP Write Lock disabled.)

In the Write Lock Position, a field technician can test installation and removal of modules without generating Traps, such as (link up, link down).

ABOUT ICONFIG (DESKTOP VERSION)

iConfig is an in-band configuration utility (in iView²) that lets users quickly and easily complete the first stages of SNMP configuration for SNMP-manageable devices. iConfig can set the IP address, subnet mask and default gateway as well as define the community strings and SNMP traps.

In addition to the above functions, iConfig offers an authorized IP address system and access restriction to MIB groups supported by manageable devices. These extra layers of security are purely optional and do not affect SNMP compatibility.

The iConfig utility can be used to upload new versions of the system software and new MIB information. It also offers diagnostic capabilities for faster resolution of technical support issues. The default user ID for both iConfig and Telnet is:

User: **admin** / Password: **admin**

The three levels of Telnet account access are:

User	Can only see status, change password and reboot
Operator	Can perform User functions and change settings
Administrator	Can perform all functions and add/delete accounts and perform the command **cleandb**

A Username and Password can be added in the **USER** tab of iConfig, or the **Accounts** command within Telnet or the Serial Configuration. Admin/admin should not be deleted until new usernames/passwords are tested. Refer to the Password section of this manual for additional information.

The iConfig utility works with the following platforms:

- Windows 2000
- Windows XP
- Windows 7
- Windows 8

The iConfig utility is available as a standalone application, as well as built in to the Windows version of iView². Both applications are included on the iView² CD. For information regarding the use of the iConfig utility, refer to the iConfig utility help file.

ABOUT SERIAL PORT CONFIGURATION

The SNMP Management Modules used with the iMediaChassis series feature a serial port that includes a DB-9 serial connector. To connect an iMediaChassis series to a terminal/computer, use a straight-through (pin-to-pin) cable. If the computer/terminal's port is not compatible with a DB-9 COM port, use the pin connection chart for reference in making a cable.) Make sure the cable length is less than 50 feet (15.24 meters). Plug one end of the cable into the DB-9 connector and the other into the appropriate port on the computer/terminal.

Set the computer/terminal for VT-100 emulation. The serial port on the computer/terminal should be set for: 38.4K baud, 8 data bits, 1 stop bit, no parity, no flow control. The F2 key functions as a **Delete** key on VT-100 emulators.

Serial Adapter Pin Connection		
RJ-45 Pin #	**DB-9 Pin #**	**Function**
5	2	Transmit (OUT)
7	3	Receive (IN)
8	5	Ground
1-4, 6	1, 4, 6 - 9	Reserved

Table 2. PIN OUTs

USING TELNET

The iMediaChassis series supports Telnet for remote configuration. All configurations that can be performed via the serial port can also be performed using Telnet (except serial passwords). Use only one Telnet session at a time. Do not use an RS-232 serial session and a Telnet session at the same time.

USING DHCP

DHCP DISABLE (STATIC IP ADDRESSING)

DHCP is disabled in the default configuration. Initially, modules are assigned a Static default IP Address of 10.10.10.10. Changes to the Static IP Address can be added manually through iConfig, an RS-232 Serial session, or Telnet. The changes will be initiated following reboot of the module

DHCP ENABLE (DYNAMIC IP ADDRESSING)

If a DHCP server is present on the network and DHCP is enabled, the DHCP client will initiate a dialog with the server during the boot up sequence. The server will then issue an IP address to the management card. Once the new IP address is received, the SNMP Management Module will reboot so that the new IP address will take effect. Refer to the *About Serial Port Configuration* for more information about Enabling/Disabling DHCP. When there is no DHCP server on the network, use iConfig or serial configuration to manually set the IP addresses.

When DHCP is enabled, the IP address (default 10.10.10.10 or user configured) is saved. When DHCP is disabled, the saved IP address will be reinstated and the device will reboot.

DHCP servers give out lease times: devices renew their leases based on the administrator-specified time. If a device cannot renew its lease, and the lease expires, the device will be given the IP address 10.10.10.10 and will reboot

MAIN SERIAL/TELNET CONFIGURATION SCREEN

After launching a serial session using a CLI (Command Line Interface) or a TELNET session, an initial self-test is performed and the main screen will display the following message: "Press **Enter** for Device Configuration." Press **Enter** for the main configuration screen, which includes the following displays:

```
Saved Values. (These values will be active after reboot)
    IP Address      - 10.10.10.10
    Subnet Mask     - 255.0.0.0                DHCP is Not Active
    Default Gateway - 0.0.0.0
    Server IP Addr  - 0.0.0.0
    New Prom File   -

Current Values. (These values are in use now)
    IP Address      - 10.10.10.10
    Subnet Mask     - 255.0.0.0
    Default Gateway - 0.0.0.0
    Server IP Addr  - 0.0.0.0
    New Prom File   -

Community String: public    Access:  r/w

Press I to enter new saved parameter values. Press P to change Password.
Press T to enter new Trap Destination. Press K to remove All Trap Destinations.
Press C to enter new Community String. Press U to remove All Community Strings.
Press E to End session. Type REBOOT to reboot unit. Press D for DHCP On/Off.
Press SpaceBar for additional commands.
-
```

Figure 1. CLI Splash Screen

Saved Values

This section displays changes made during current session:
• IP Address (MUST be assigned during initial configuration)
• Subnet Mask (MUST be assigned during initial configuration)
• Default Gateway

Current Values

This section displays values currently in use:
- IP Address (IP address of SNMP agent)
- Subnet Mask (mask to define IP subnet agent is connected to)
- Default Gateway (default router for IP traffic outside subnet)

Command List

This section displays the commands available:
- **I** = Enter New Saved Parameter Values
- **P** = Change Password
- **T** = New Trap Destination
- **K** = Remove ALL Trap Destinations
- **C** = New Community String
- **U** = Delete ALL Community Strings
- **D** = Enable/Disable DHCP
- **E** = End Session
- **Space Bar** = Device Specific Configuration commands

NOTE
Reboot after making any modifications to the saved parameter values or the changes will not take effect. To reboot, type **Reboot** at the prompt on the main configuration screen, or turn the chassis **OFF** then **ON** again by turning off the switches on the back of the power supplies, or reseat the module.

ASSIGNING IP INFORMATION

To modify the saved parameter values (i.e., assign IP address and subnet mask), press **I**. Enter the IP address and subnet mask for the connected device, pressing **Enter** after each. The default gateway can also be assigned, if desired (press **Enter** to skip).

When finished, press **Enter**, then type **reboot** for changes to take effect. The Saved Values and Current Values should now display both the changes made (e.g., new IP address and subnet mask).

CREATING COMMUNITY STRINGS FOR SNMP

The purpose of community strings is to add a level of security to a network. The default community string is named "public" and has read/write access. Do not delete the community string “public” until the new community string has been tested. Add necessary custom community strings such as one with read/only access (for general use), the other with read/write access (for the administrator).

To create a new community string, go to the main configuration screen and press **C**. Enter the name of the new community (up to 16 characters, no spaces) and press **Enter.** Then type one of the following to assign the community string's access rights:

R/O = read-only access
R/W = read/write access
Enter = abort

Press **Enter**. When finished, press **Enter**, and type **reboot** for changes to take effect. The Saved Values and Current Values should now both display the changes made (e.g., new IP address and subnet mask). iConfig MIB definitions allow the user greater control of Community Strings than serial or telnet.

DELETING COMMUNITY STRINGS

To delete all community strings (except the default, “public”) and start over, press **U**. Press **Y** to delete all strings or **N** to abort. Then, press **Enter.** This function will delete ALL community strings. To selectively delete community strings, use iConfig.

ASSIGNING TRAP DESTINATIONS

A manageable device sends traps when a certain events take place. To enter a trap destination, press **T**. Enter the IP address of the destination device and press **Enter**. Then, type the name of the community string (that the destination device has been configured to accept) and press **Enter**. This function enables ALL of the traps. To selectively activate and deactivate traps, use iConfig. iConfig Traps allow greater control using the Trap Edit than the serial and Telnet does. To choose generic or enterprise-specific Traps, use iConfig.

REMOVING TRAP DESTINATIONS

To remove all trap destinations, press **K**. Press **Y** to remove all trap destinations. Press **N** to abort and then press **Enter**.

CHANGE SERIAL PASSWORD

The serial configuration does not have a default password; it is optional.

Password-protect the serial configuration process by pressing **P** from the main configuration screen. Type the password and press **Enter**. Passwords are case sensitive and should be no more than eight characters in length, with no spaces. This password will be requested whenever logging on or off. To remove password protection, select **P** and instead of entering a password, press **Enter**.

ENABLING/DISABLING DHCP

To Enable/Disable DHCP, press **D** and then type reboot for the changes to take effect. Refer to the About DHCP section of this manual for more information.

ENDING A SESSION

When ending a session, press **E** before disconnecting the cable in order to stop the device from continuing to send feedback status through to the serial port. If a session is not ended properly, the Telnet session cannot be launched.

DEVICE-SPECIFIC OPTIONS— DOWNLOADING FILES

With the iMediaChassis series, firmware can be downloaded from a central server via a TFTP protocol. Initiate this download via serial configuration or Telnet session. Make sure the IP Address and the name of the file being downloaded are correct in the Current Values section of the Main Configuration screen. To download a file, press the **Space Bar** in the Command List section of the Main Configuration screen (serial configuration). Type **download** and press **Enter** to be taken to the Download a File screen. This screen displays the IP Address of the TFTP server and the name of the file. Press **Enter** to start downloading the file.

If the download is interrupted, do not reset the module or reboot the SNMP Management Module; doing so can corrupt the PROM and render the module useless. Close the session and then open a new TFTP session.

ADDITIONAL DEVICE-SPECIFIC OPTIONS

The iMediaChassis series also includes device-specific options. Press the **Space Bar** when in the Command List section of the Main Configuration screen (serial configuration/Telnet session), type the name of the action, and press **Enter**.

```
Command         Description
--------        -----------
tasks           Display Task List
memory          Display Memory Usage
cleandb         Reboot With Clean Database
download        File Download
version         Show Firmware Version
reboot          Reboot Unit
sysdescr        Change System Descriptions
accounts        Add or Delete Username/Password Accounts
modules         Display Modules Status

->
Press RETURN To Go Back To Main Screen.
```

Figure 2. Command List

tasks Displays the task list with priorities.

memory Displays the memory usage

cleandb Removes all information in the database, except the IP address of the device.

Download Opens the Download dialog box where the firmware is located and can be downloaded via the server address. The Server IP Addr must be entered in the Main Configuration screen using TFTP protocol.

version Displays the PROM version and build date

reboot Reboots the unit

sysdescr Allows the editing of sysName, sysDescr, and Port information text.

accounts Allows management of Usernames/Passwords account. Administrators must maintain a password list.

modules Displays a list of installed modules including the slot location.

SOFTWARE INSTALLATION

All the options available through the Serial/Telnet session and more is available when using the software GUI of iView². The GUI is offered as a Desktop or Webserver version; both can be downloaded at the www.advantech-bb.com website. Please note, however, that any new managed products after January of 2017 will not be supported in the Desktop version.

USING IVIEW²

iView² is a network management application for B+B SmartWorx' intelligent networking devices. It features a Graphic User Interface (GUI) and gives network managers the ability to monitor and control products from a variety of platforms. The software is a free download, and available in a Desktop versions and a Webserver version.

USING IVIEW² DESKTOP VERSION WITH HP OPENVIEW

During the installation, the iView² application will ask if HP OpenView is installed on the management PC. Click **Yes** to integrate the appropriate files. Once in OpenView, highlight the media converter icon and select the media converter; OpenView will then launch iView².

SYSTEM REQUIREMENTS

To run iView², the management PC must be equipped with the following:

- 29 MB free disk space, 64 MB RAM
- Windows NT 4.0 Service Pack 5, 2000 Professional, XP Professional
- Microsoft SNMP Services Installed
- Microsoft IE 4.0 or Higher

iView² is a network management application for B+B SmartWorx' intelligent networking devices. It features a GUI, which provides network managers the ability to monitor and control B+B SmartWorx' products. The application is available as a free download on the website and can also function as a snap-in module for HP OpenView Network Node Manager and other NMS application

iView² Desktop version supports the following platforms:

- Windows 2000
- Windows XP
- Windows 7
- Windows 8

iView² Webserver version requires the following:

- MySQL 5.1 or higher
- Apache/TomCat 6 or greater
- JAVA ver 1.7 or greater

Browsers required:

- MS Internet Explorer v 10 or greater
- Mozilla Firefox v 15.0 or greater
- Google Chrome v 35 or greater

OTHER NMS APPLICATIONS

If using an application other than iView² for management, integrate the SNMP MIBs into the vendor's NMS application. The MIBs II are located in the MIB folder, a subdirectory of iView². If using the Webserver version of iView² , on your PC's hard drive, go to Program Files\Apache Software Foundation\Tomcat_6_0\webapps\iView3\MIBS. **Be advised that unless you have an actual managed product connected to the network, that iView² identifies, you will not be able to locate the MIBs files.**

Refer to your application's documentation for information on how MIB files are integrated when not using iView²; MIBs II are based on standard RFC 1213.

USING IVIEW² WEBSERVER VERSION

iView² is also available as a Webserver version. This is a browser-based software, also downloadable from the www.advantech-bb.com site. It offers more features than the Desktop version, such as supporting hundreds of users and particular B+B SmartWorx (formerly IMC Networks) manageable fiber devices. It still offers MIBs II and levels of security.

Refer to the "*Getting Started*" document and "*Installation Instructions*" documents that are included with the Webserver download in the zip file, posted on the website. The rest of this manual addresses the Desktop Version for software options.

UPDATE MANAGER:DESKTOP VERSION

iView² offers the option of scheduling an update search for B+B SmartWorx" devices listed in the Network outline. Within iView², select **Tools/SNMP Options** from the navigation toolbar. Select **Update Manager Options**, and a dialog box will be displayed, in which you can select when to run the update search. This option enables the end user to determine if they have the latest firmware, and download the latest if they do not. It does not automatically run the download, so the end user can review the release notes included with the binary file, and decide whether to download it or not.

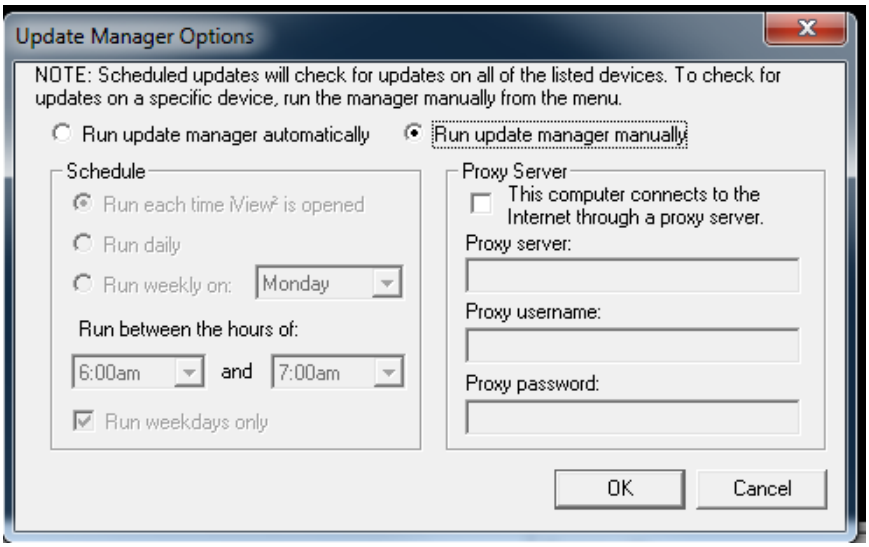

Figure 3. Update Manager

In the Webserver version, similar options are offered. Refer to the "Getting Started" document that is included with the Webserver download in the zip file, posted on the website.

FILE MANAGEMENT FOR UPGRADING PROM (DESKTOP VERSION)

The following screen, located in the iConfig utility of iView², shows the File Management functionality of the Unified Management Agent. Operators can easily upload and store new firmware versions for upgrading multiple devices with on-board logic installed in, or connected to, an iMediaChassis series.

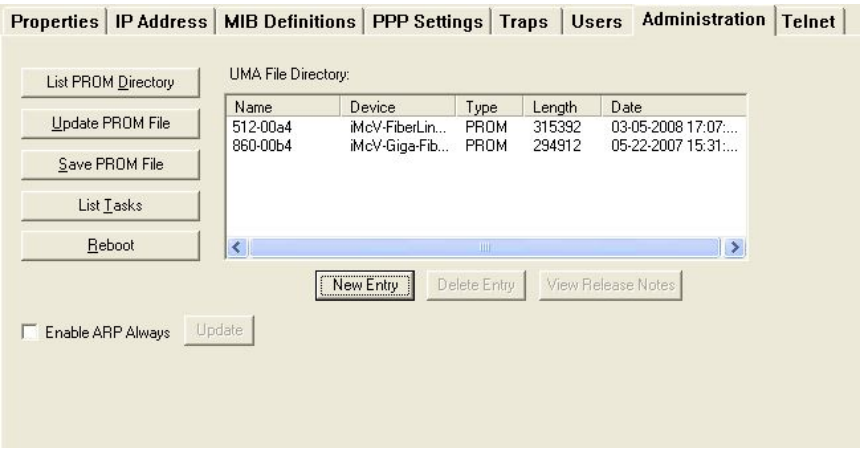

Figure 4. iCONFIG SECTION

UMA (Unified Management Agent)

Centralized management makes practical sense for networks of all sizes, especially service provider networks that must monitor and upgrade large quantities of devices. The Unified Management Agent (UMA) allows operators to manage all IMC modules with Flash PROM (FiberLinX-II series) installed in a B&B Electronics' iMediaChassis series, with a single IP address from a central location. In addition, UMA allows users to centrally manage and administer firmware upgrades over multiple devices.

For example, install 20 iMcV-FiberLinX-II devices in a 20 slot iMediaChassis at the Central Office (CO) then connect each to a remote iMcV-FiberLinX-II or AccessEtherLinX unit installed at the customers premise (CPE); UMA will then allow users to manage all 41 devices (including the chassis at the CO) via a single IP address. Users may still assign IP addresses to each iMcV-FiberLinX-II and manage them independently when the SNMP Management Module within the iMediaChassis is omitted.

When an SNMP request for an iMcV-FiberLinX-II comes in, the SNMP Management Module in the iMediaChassis series passes the request to the SNMP agent in the specific module. The SNMP agent in the iMcV-FiberLinX-II provides the relevant management information, which is then routed via the SNMP Management Module and supplied to the client GUI (iView², version 1.8 or higher), as well as the serial port and Telnet.

EASY UPGRADES WITH THE UNIFIED MANAGEMENT AGENT (UMA)

- Upgrade one or multiple Host (CO) or Remote (CPE) devices with just a few mouse clicks. Refer to the iMcV-FiberLinX-II, iMcV-GigaFiberLinX, AccessEtherLinX and IE-Mini FiberLinX-II series manuals for complete information.
- All devices in chassis are fully functional while upgrades are in process.
- Manage up to 41 devices with a single IP address.
- Telnet access and view for all system devices.
- Only one Ethernet port is required, reducing the number of ports used on a network switch.

TELNET SESSION AND UMA (UNIFIED MANAGEMENT AGENT)

With the Unified Management Agent, users can also manage multiple devices installed in, or connected to, an iMediaChassis via a Telnet session, as well as assigning an IP address.

In the example below, the devices listed on the left (e.g. MetroFiber 3 represent Host iMcV-FiberLinX-II units while the devices listed on the right (Irvine POP 3) represent Remote iMcV-FiberLinX-II units. The names (SNMP sysName) given to each iMcV-FiberLinX-II device are easily assigned/ changed via iView², serial configuration, etc.).

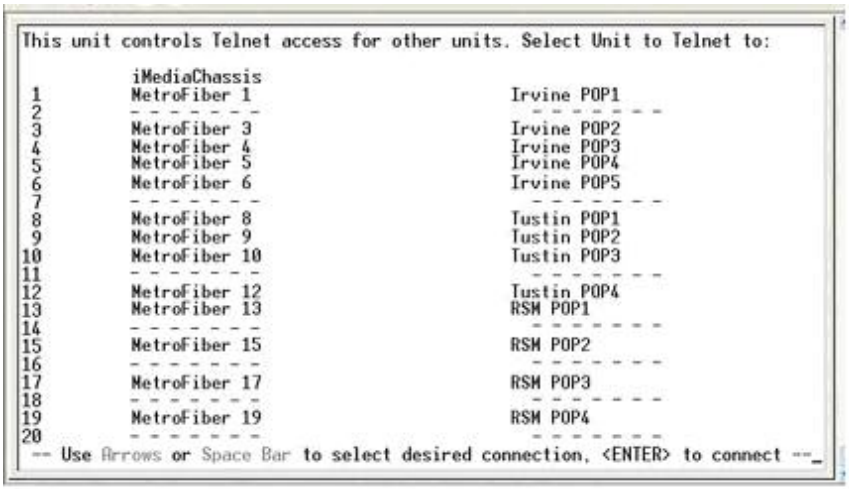

Figure 5. Telnet Session

The FiberLinX-II series modules offer a mode of saving a Configuration File, as well as a Restore File option. Please refer to the appropriate manuals for complete information.

In the CLI or Telnet session, you can enter a server IP address that you have assigned to upload whatever version of firmware you want to distribute to your customer base, instead of instructing them to go to the vendor's website or sending out multiple emails with the binary file attached.

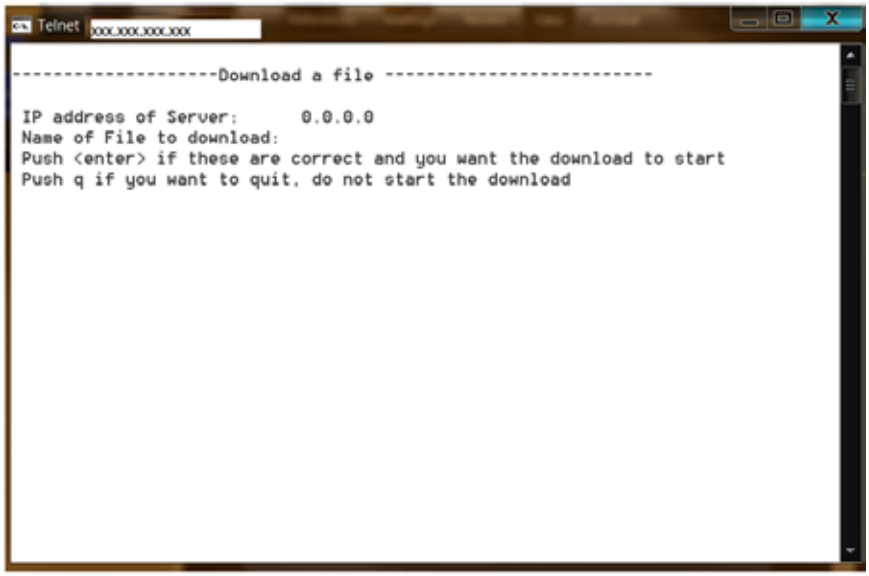

Figure 6.File Download

PASSWORDS

Passwords are a way to make the management of network devices secure. If the Serial password is lost, download the latest version of the binary file and load it through the iConfig utility. Any serial password entered will be removed, and there will be no password for the console session.

The **Desktop version** of iView² allows a password of between 1 and 8 characters long; the password can consist of a combination of any ASCII characters except spaces, and passwords are case sensitive.

The **Webserver version** of iView² allows a password of at least 3 characters long and no more than 60 characters. Passwords can contain a-z, A-Z, and 0-9 characters. Password cannot be the same as User name. Password cannot contain the User Name.

If the username/password is lost in iConfig, launch a HyperTerminal session to access the CLI. Once the boot sequence is complete, press the **Space Bar** and then type in the command **cleandb**. This will reset the username/password back to admin/admin. If BOTH password accesses are lost, contact **Technical Support**

SPECIFICATIONS

Environmental -- Intended for indoor and outdoor use.	
Operating Temperature	32° - 122° F (0° - 50° C)
Storage Temperature	21° - 160° F (-6° - 71° C)
Operating Humidity	5 - 95% (non-condensing)
Power Consumption	Typical @ 5V
	600mA

Table 3. Specifications

CERTIFICATIONS

UL/CUL: Listed to Safety of Information Technology Equipment, including Electrical Business Equipment.

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (2004/108/EC) and the Council Directive on Electrical Equipment Designed for use within Certain Voltage Limits (2006/95/EC). Conforms to UL Std. 60950-1; Certified to CSA Std. C22.2 No. 60950-1

FIBER OPTIC CLEANING GUIDELINES

Fiber optic transmitters and receivers are extremely susceptible to contamination by particles of dirt or dust, which can obstruct the optic path and cause performance degradation. Good system performance requires clean optics and connector ferrules.

Use fiber patch cords (or connectors, if you terminate your own fiber) only from a reputable supplier; low-quality components can cause many hard-to-diagnose problems in an installation.

Dust caps are installed at B+B SmartWorx to ensure factory-clean optical devices. These protective caps should not be removed until the moment of connecting the fiber cable to the device. Should it be necessary to disconnect the fiber device, reinstall the protective dust caps.

Store spare caps in a dust-free environment such as a sealed plastic bag or box so that when reinstalled they do not introduce any contamination to the optics.

If you suspect that the optics have been contaminated, alternate between blasting with clean, dry, compressed air and flushing with methanol to remove particles of dirt.

ELECTROSTATIC DISCHARGE PRECAUTIONS

Electrostatic discharge (ESD) can cause damage to any product, add-in modules or stand-alone units, containing electronic components. Always observe the following precautions when installing or handling these kinds of products:

Do not remove unit from its protective packaging until ready to install.

Wear an ESD wrist grounding strap before handling any module or component. If the wrist strap is not available, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.

Hold the units by the edges; do not touch the electronic components or gold connectors.

After removal, always place the boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the modules or stand-alone units over any surface.

WARNING! Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.

CERTIFICATIONS

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (2004/108/EC). For further details, contact B+B SmartWorx.

Class 1 Laser product, Luokan 1 Laserlaite,
Laser Klasse 1, Appareil A'Laser de Classe 1

European Directive 2002/96/EC (WEEE) requires that any equipment that bears this symbol on product or packaging must not be disposed of with unsorted municipal waste. This symbol indicates that the equipment should be disposed of separately from regular household waste. It is the consumer's responsibility to dispose of this and all equipment so marked through designated collection facilities appointed by government or local authorities. Following these steps through proper disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about proper disposal, please contact local authorities, waste disposal services, or the point of purchase for this equipment.

ADVANTECH B+B SMARTWORX TECHNICAL SUPPORT

Phone: **1-800-346-3119**
(Monday - Friday, 7 a.m. to 5:30 p.m. CST)
Fax: **815-433-5109**
Email: support@advantech-bb.com
Web: www.advantech-bb.com

Document: #:50-80950-01_A3 _1017