



Napco Access Pro is a division of Napco Security Technologies Inc.
(Nasdaq Symbol: NSSC) consisting of Access Control Brands
Continental Access and E-Access

Continental **Access**
A Napco Security Group Company

CA4K[®]

CardAccess Software

UniVerse Finder Utility Software Programming Guide

(For use with V1.5.0.1 or later, non x-port devices)

Supported Controllers

uniVerse (CICP2100 & CICP2100S)
duoVerse (CA-2)
Super Two (CICP1300 w/ CICP1300NETBD2)
Accelaterm (CICP2800 w/ CICP2800NETBD2)
Accelerator (CICP1800 w/ CICP2800NETBD2)

NAPCO Security Technologies Inc.
355 Bayview Avenue, Amityville, NY 11701
Telephone: 631-842-9400 Fax: 631-842-9135
www.NapcoAccessPro.com

Publicly traded on NASDAQ Symbol: NSSC

DISCLAIMER

Napco Access Pro makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Napco Access Pro reserves the right to revise this publication and to make changes in the content hereof without the obligation of Napco Access Pro to notify anyone of such revision or changes.

Copyright © 2024 by Napco Access Pro. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or stored in a retrieval system, without the prior written permission of:

Napco Access Pro
355 Bayview Avenue,
Amityville, NY 11701
Telephone: 631-842-9400
FAX: 631-842-9135

This document contains proprietary information about NAPCO Security Technologies. Unauthorized reproduction of any portion of this manual without the written authorization of NAPCO Security Technologies is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. NAPCO Security Technologies assumes no responsibility for incorrect information this manual may contain.

A NAPCO SECURITY TECHNOLOGIES COMPANY

Publicly traded on NASDAQ Symbol: NSSC

Visit our websites:

<https://www.napcoaccesspro.com/>

<https://www.napcosecurity.com/>

<https://www.alarmlock.com/>

Must Read before you begin installation

- The **CardAccess.uniVerseFinder.exe** utility software is not used for programming Lantronix X-Port devices. However, using the uniVerse Finder, if you select **Other Devices** and search, you will be able to see if your device is a Lantronix X-port, as its Device Type will show up as **(X5)**. For programming Lantronix x-port ethernet adapters please use the Lantronix “**Device Installer**” software to configure.
- The UniVerse Finder Utility software must be version **V1.5.0.1 or later**. The latest version of UniVerse Finder Utility is included with CA4K. After CA4K is installed, the UniVerse Finder Utility program can be found on your PC in the following folder:
C:\Program Files(x86)\CardAccess4K\Tools.
You can also download the latest uniVerse Finder Utility by going to tech.napcosecurity.com, posted under **Software Downloads > Napco Access Pro**
- If using the new ethernet adaptors **CICP1300NETBD2/CICP2800NETBD2** you must use ethernet firmware version **17.7.7** or later. If using a uniVerse (CICP2100 / CICP2100S) the latest firmware is **12.8.2** or later.
- All ethernet adapter’s default to DHCP mode. A DHCP enabled router is recommended to provide an IP address to the ethernet adapters. Upon obtaining an IP address from DHCP, it is recommended to program in a static IP address that must never change. Please contact your network administrator for a static IP address.
- The computer with the UniVerse Finder Utility must be on the same subnet as the IP address provided by the DHCP enabled router.
- To **RESET (clear)** any previously programmed IP address information, and to Reset the log in credentials, you must follow the instructions in Appendix for your device/controller.
- The UniVerse Finder Utility also contains a web utility that should not be used. It is executed by clicking the **Launch Web** button. The Web utility is only for the CICP2100/CICP2100S controllers with older firmware 12.6.8 or earlier.

Prerequisites

- A functional CA4K System (version 1.1.x or later).
- DHCP enabled Router.
- Mac Address of the Ethernet Network Adapter
- UniVerse Finder (NLM Configuration) utility Version **1.5.0.1** or later

Network Wiring Diagram

Supported Controllers (non Lantronix X-Port Devices)

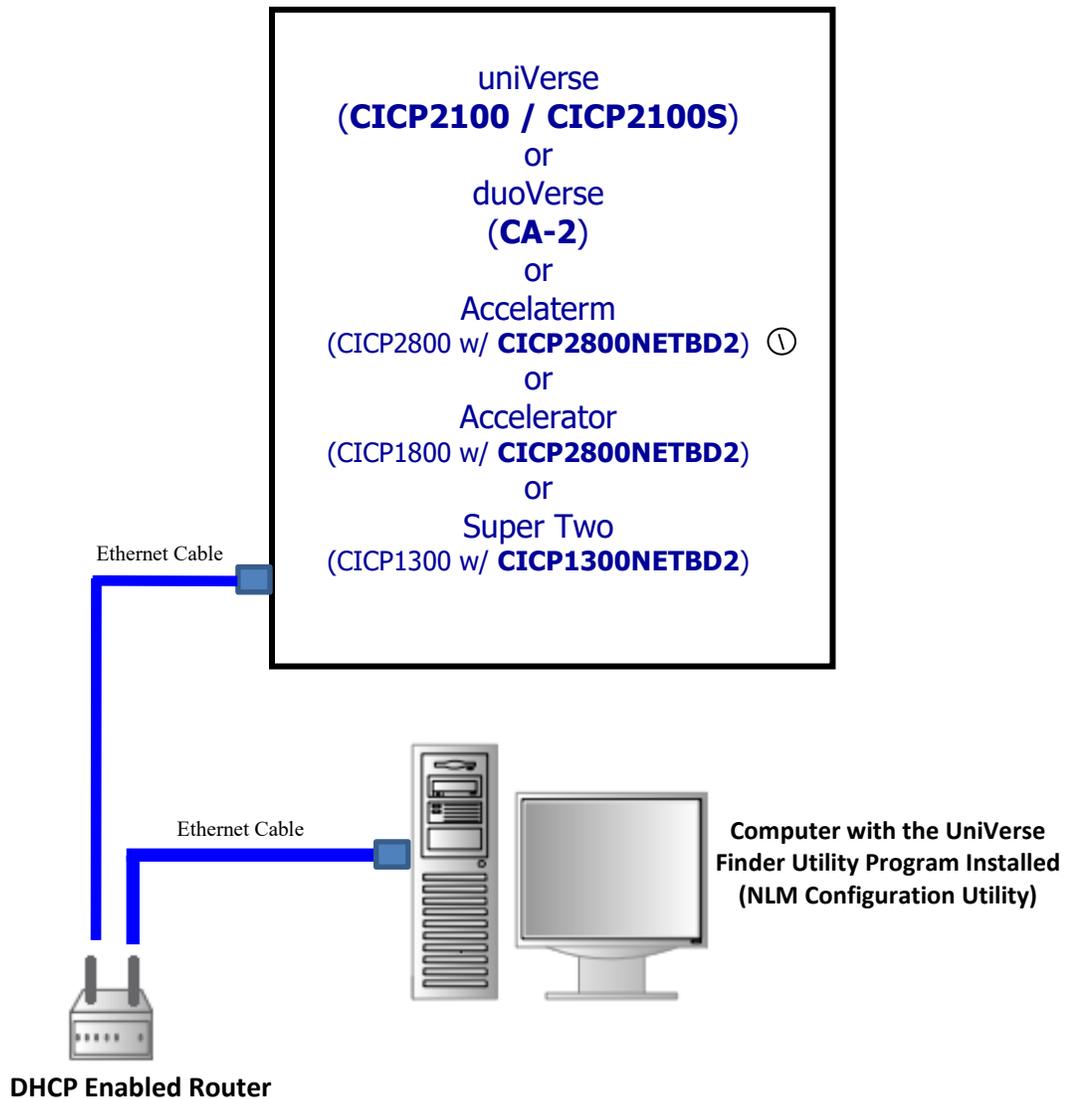


Figure 1.

Getting Started

1. Verify your ethernet adaptor is a non Lantronix X-Port device. If not done so already, install the **CICP2800NETBD2/CICP1300NETBD2** on the Accelaterm / Accelerator or Super Two controller main board (refer to **WI2434** for the CICP1300NETBD2 and the **WI2543** for the Accelaterm / Accelerator for specific information on how to physically install the modules).
2. Using an ethernet cable, connect your ethernet network adapter or Controller to a DHCP enabled router (refer to Figure 1 above).
3. Power up the controller. The ethernet adaptors will default to DHCP mode and will request and obtain an IP address from an available DHCP server. If a DHCP server is not found, an APIPA address will be assigned to the **adaptors**. An APIPA IP address is in the range of 169.254.x.x.

Configuring the Controllers

The latest version of UniVerse Finder Utility is included with CA4K. After CA4K is installed, the UniVerse Finder Utility program can be found on your PC in the following folder:

C:\Program Files(x86)\CardAccess4K\Tools.

You can also download the utility by going to tech.napcosecurity.com, under **Software Downloads > Napco Access Pro**

1. Locate the **CardAccess.UniVerseFinder.exe** program. If you downloaded the utility and the folder has not already been extracted, **right-click** the downloaded zip file and select **“Extract All”** to a local folder of your choosing. Inside the extracted folder or in the Tools folder, right-click the file named **CardAccess.UniVerseFinder.exe** and click **Run as Administrator**.
2. Upon launching the utility, the **uniVerse Controller IP Search** screen will display.
3. On this screen, select **Controllers** and click **Discover** (refer to Figure 2).
4. Upon clicking the **Discover** button, the middle of the screen will display the devices found. Each device will display the Mac Address and IP Address of the devices found (refer to Figure 3).

Note: The status bar will also display the number of devices found (**n device(s) found**).

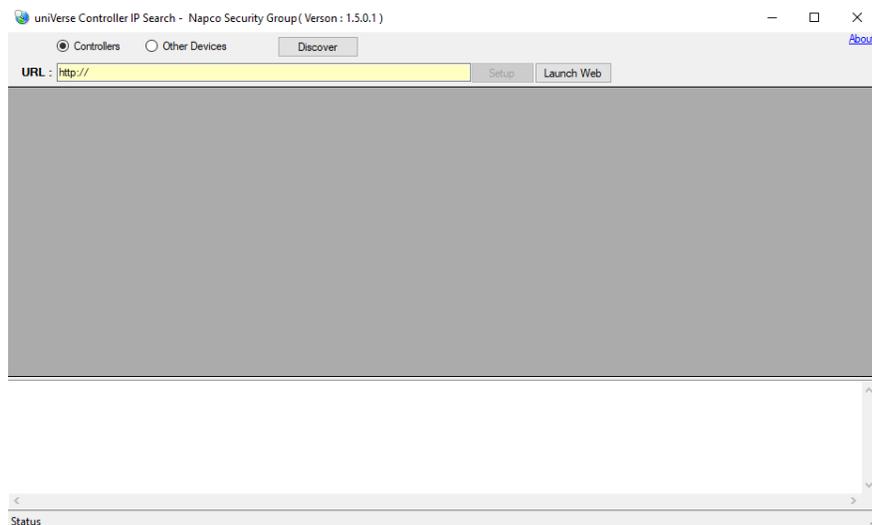


Figure 2.

7. On the **NLM Configuration Setup** page, view the **Selected NLM** information. The MAC Address must match the MAC address on the controller you are trying to discover (refer to Figure 6). The IP address must match the **Device IP address** on the **NLM Configuration** page.



Figure 6.

8. By default, the ethernet adaptors will all default to DHCP. The Device IP Address is provided by DHCP (refer to Figure 15). If it displays DHCP, you must change it to **Static** and program in a Static IP Address.

VERY IMPORTANT: The IP Address of the device must never change. Please contact the Network Administrator for the static IP information.

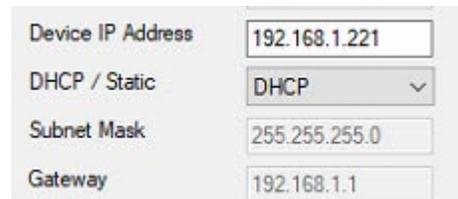


Figure 15.

Programming in a Static IP Address, Subnet Mask and Gateway

1. To program in a static IP Address, select **STATIC** in the DHCP/Static dropdown list.
2. Type in the Static IP Address, Subnet Mask and Gateway. (Connection Timeout you can leave at default)
3. Upon entering the Static IP information, click **the Write Config** button.

Note: For our demonstration, we will use the same IP address of 192.168.1.221 and set it to **STATIC** (refer to Figure 16). Again, please contact the Network Administrator to get a static IP address.

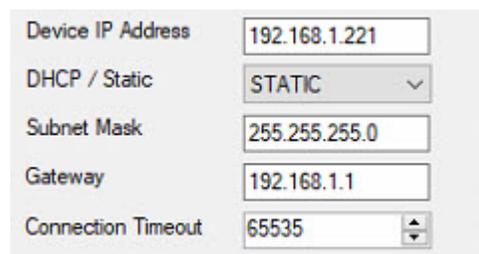


Figure 16.

Programming Baud rate, Port number, Operation Mode, and AES setting

1. Select a **Baud Rate**. If you are not using repeat mode, you can select the maximum baud rate for your Controller / ethernet adaptor and proceed.

Note: When selecting the Baud Rate, it is especially important to know the maximum baud rate for each controller. If you are not using repeat mode, you can select the maximum baud rate for your ethernet adaptor and proceed (Refer to Maximum Baud Rate Chart below). If you are using Repeat Mode, all the baud rates must match the baud rate of the lowest maximum baud rate in the chain. Mixing high-speed baud rates with a baud rate lower than 115,200 is not supported, as high-speed controllers will only operate at a minimum of 115,200 baud. If a Turbo Superterm or Superterm control panel is included in the network, it must be equipped with the Continental Accelerator Board (CICP18ACCB) along with the CICP2800NETBD2 for the higher baud rates. **Note that the Continental *Super Two*, *Smarterm*, *Miniterm*, and *Microterm* control panels should not be included in a chain with other high speed baud rates.**

2. **Server Port** number. The default for all controllers is **3001**.
3. **Operation mode**. Set to **Legacy**
4. **AES Encryption Type**. Default is none. (AES 128-Bit is improved with CA4K 1.2.x or later. If using AES 128 Encryption type, it needs to be set to 128-bit in the UniVerse Finder. If setting the type to 128-bit, when configuring your com ports in CA4K 1.2.x, you must also set security type to AES128. Refer to AES Encryption Support Chart below.
5. **Cloud Settings**. Leave the settings at the default value. Saved for future use.
6. Upon entering the Baud Rate, Server Port number or AES Encryption Type, click **the Write Config** button.

Maximum Baud Rates

Model #	Maximum Baud Rate Supported
uniVerse (CICP2100 / CICP2100S)	921.6 K (High Speed)
duoVerse (CA-2)	921.6 K (High Speed)
Accelerator w/ CICP2800NETBD2	921.6 K (High Speed)
Accelerator Board w/ CICP2800NETBD2	921.6 K (High Speed)
Super Two w/ CICP1300NETBD2	57.6 K
Legacy Turbo Superterm w/o Accelerator Board	57.6 K
Legacy Superterm, Smarterm, Miniterm & Microterm	19.2 K

AES Encryption

Model #	AES 128-Bit Support
uniVerse (CICP2100 / CICP2100S)	Yes, supports firmware 12.8.2 or greater
duoVerse (CA-2)	Yes, supports firmware 12.8.2 or greater
Accelerator w/ CICP2800NETBD2	Yes, supports firmware 17.7.7 or greater
Accelerator Board w/ CICP2800NETBD2	Yes, supports firmware 17.7.7 or greater
Super Two w/ CICP1300NETBD2	Yes, supports firmware 17.7.7 or greater
Legacy Superterm, Smarterm, Miniterm & Microterm	Not Supported

Read Config / Write Config buttons

To retrieve the current settings from your ethernet adaptors, click the **Read Config** button. The information retrieved will be displayed in the text box. To write the settings to the ethernet adaptors, click the **Write Config** button.

1. Upon clicking the **Read Config** or **Write Config** buttons, it will take a minute to perform the command and reboot the device (refer to Figure 13).
2. Upon clicking the Read Config or Write Config buttons, the data retrieved or written to the device will display in the text box (refer to Figure 14).

Very Important: If the data in the text box is **RED**, this represents an **ERROR**. Please read the text carefully to determine what went wrong.

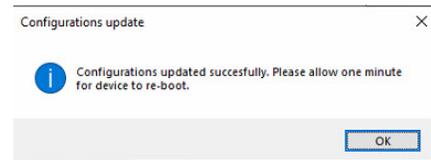


Figure 13

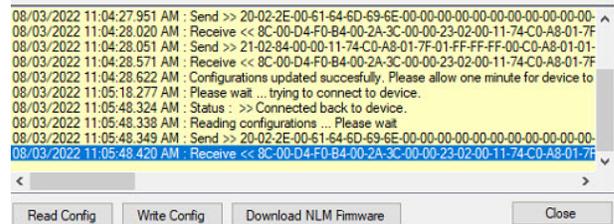


Figure 14

Logging into the Controllers

1. To communicate with the **ethernet adapters**, you must log into the device (refer to Figure 7). By default, the default Login credentials will populate. The default log in credentials is **User = admin and Password= admin**. If you wish to change the default credentials, refer to step 2 below.

Figure 7.

2. To change the Username and Password in the device, enter the new Username and Password and click the **Write Config** button (refer to Figure 8).

Note: The next time you log in to communicate to the device as per Figure 7, you must use the new credentials.

Figure 8.

How to Update your Firmware

The **Download NLM Firmware** button allows you to update the firmware of your Controller's ethernet adaptor or Controller. To determine the latest available firmware version for your ethernet adaptors or controllers, look in the CA4K Firmware folder or in the downloaded uniVerse Finder Utility zip folder. If there is newer firmware available in the folder, it will list the next revision sequentially, such as *con17_7_7_8*. If the firmware is not displaying or is not up to date, refer to the following steps to update.

Note: If using a **CICP1300NETBD2** or a **CICP2800NETBD2** verify the firmware version is displaying **17.7.7** or later (refer to Figure 9.) If using a uniVerse (**CICP2100 / CICP2100S**) you must use firmware **12.8.2** or later.

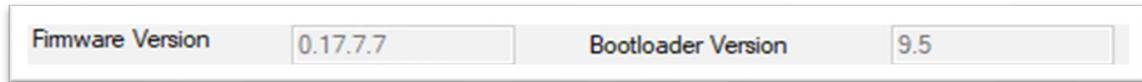
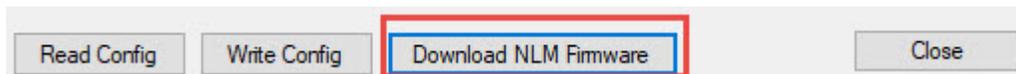


Figure 9.

1. To download updated NLM Firmware, click **Download NLM Firmware** button.



2. On your PC navigate to *c:\program files (x86)\CardAccess4K\Firmware* folder or navigate to the downloaded uniVerse Finder Utility zip folder and select the latest firmware file. Click **Open** (refer to Figure 11).

Note: For example, if there is a newer firmware available, it would display the next revision sequentially such as *con17_7_7_8*

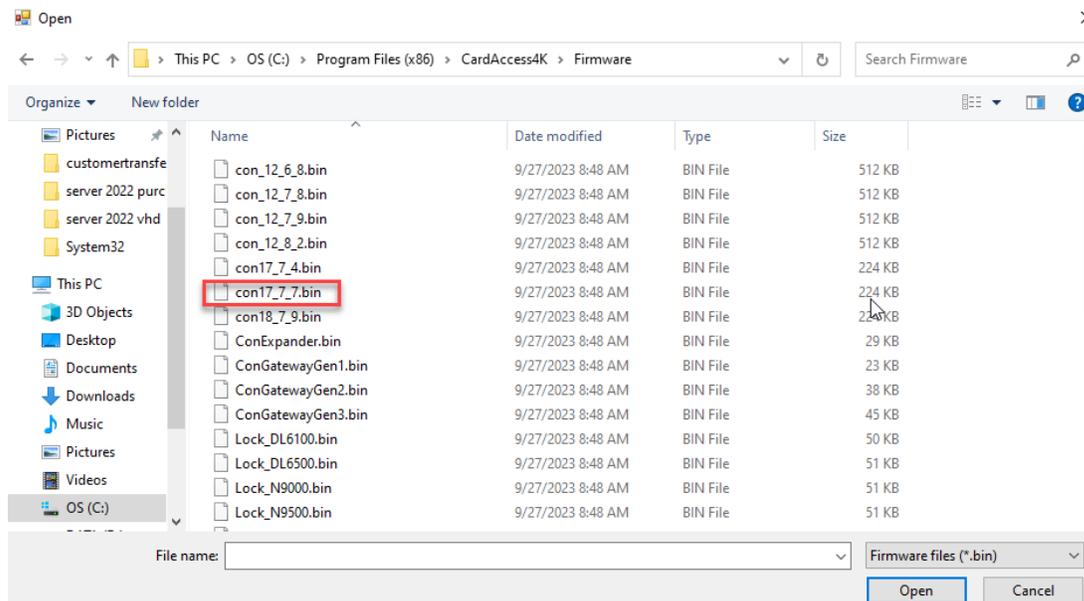


Figure 11.

3. Upon clicking **Open**, the firmware file will start downloading (this may take a few minutes). Upon the completion of the Firmware download, a **Firmware Updated Successfully** message will display (refer to Figure 12).

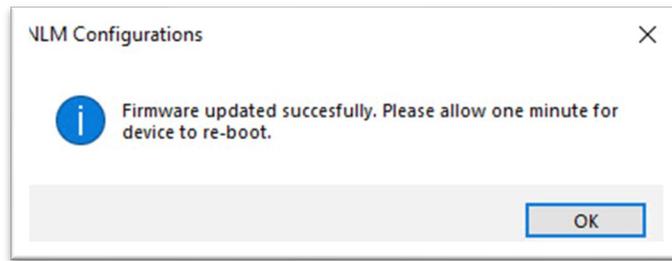


Figure 12.

Programming Peer-to-Peer Lockdown (Optional Feature)

The **Lockdown Settings** is used for the Peer-to-Peer Lockdown feature only. The Peer-to-Peer lockdown feature is only supported on the **CICP1300NETBD2** and **CICP2800NETBD2**.

The steps to configure Peer-To-Peer lockdown using CA4K are explained in detail, in **WI2544**. You do not need to change the optional settings, if the Peer-to-Peer lockdown feature, is not going to be used,

1. To configure the Peer-to-Peer Lockdown feature, click **Change** (refer to Figure 19).



Figure 19.

2. Upon clicking **Change**, the **Lockdown Settings** configuration screen will display. You will need to enter the Panel IP Addresses of the other controllers that are going to be used in the lockdown area. In the Panel IP Address, enter the IP address of the Panel(s) and click **Add** (Refer to Figures 20). After the IP Addresses are populated, Press **Write**

Note: Repeat the above steps for each Panel that will have a Lockdown control reader on it.

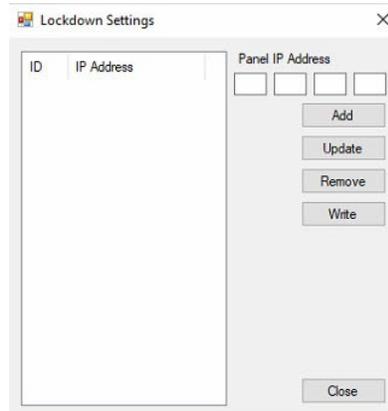


Figure 20.

APPENDIX A – Reset Procedure for CICP1300NETBD2 (Super Two)

JP4 (Configure for DHCP Request)

The following procedure is used to clear the current IP address information and configure for DHCP

1. Move Jumper JP4 to positions 2-3.
2. Cycle power to Super Two.
3. Wait 30 Seconds, the Green/Red LEDs stop flashing
4. Restore Jumper JP4 to positions 1-2.
5. The Super Two should obtain a new IP address from DHCP.

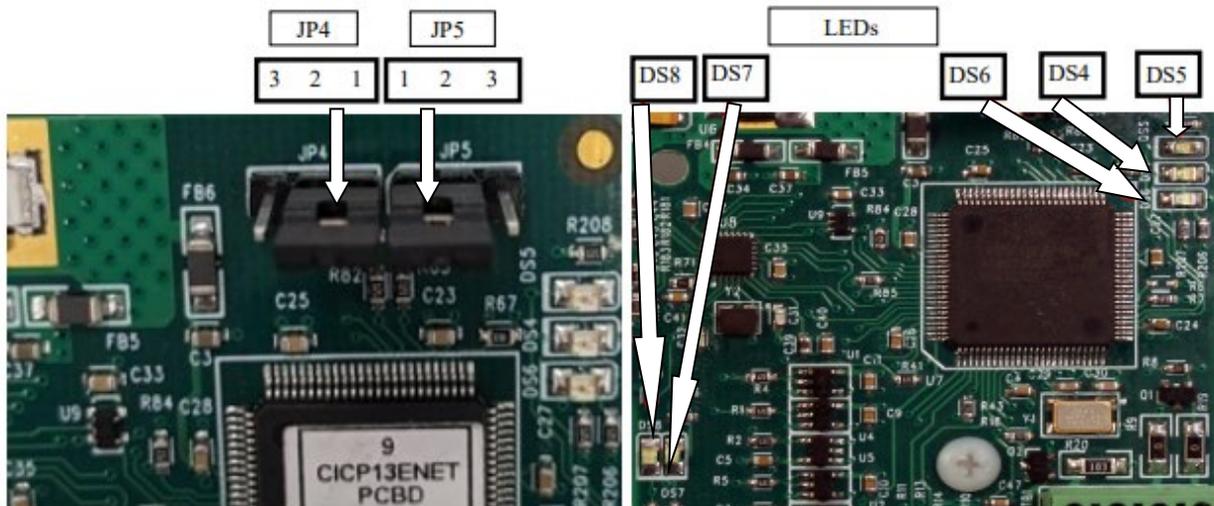
JP5 (Reset Universe Finder Utility Username and Password)

The following procedure is used reset the Universe Finder utility Username and Password back to the default of "admin" and "admin"

1. Move Jumper JP5 to positions 2-3.
2. Cycle power to Super Two.
3. Wait 30 Seconds, the Green/Red LEDs stop flashing
4. Restore Jumper JP5 to positions 1-2.
5. The Universe Finder Utility Username and Password is reset to "admin" and "admin".

Jumper Settings	
Jumper	Function
JP4	1-2 Normal Location (as shown)
	2-3 Used to clear the current IP address information and configure for DHCP
JP5	1-2 Normal Location (as shown)
	2-3 Used to Reset Universe Finder utility Username and Password to "admin" and "admin"

LED Functions	
LED	Function
DS4	Fast Blink = Firmware is in bootloader Slow Blink = Application is running Off/On = Micro is not running
DS5	Fast Blink = Firmware is in bootloader Solid On = DHCP is searching for IP Off = IP address obtained
DS6	On = Static IP Configured Off = Static IP Not Configured
DS7	On = Ethernet Connected Fast Blink = Ethernet is communicating
DS8	10/100 Link Operating Speed Indication ON = 100Mbps OFF = 10Mbps



APPENDIX B – Reset Procedure for CICIP2800NETBD2 (Accelterm / Accelerator)

JP4 (Configure for DHCP Request)

The following procedure is used to clear the current IP address information and configure for DHCP.

1. Move Jumper JP4 to positions 2-3.
2. Cycle power to Accelterm.
3. Wait 30 Seconds, the Green/Red LEDs stop flashing
4. Then Restore Jumper JP4 to positions 1-2.
5. The Accelterm should obtain a new IP address from DHCP.

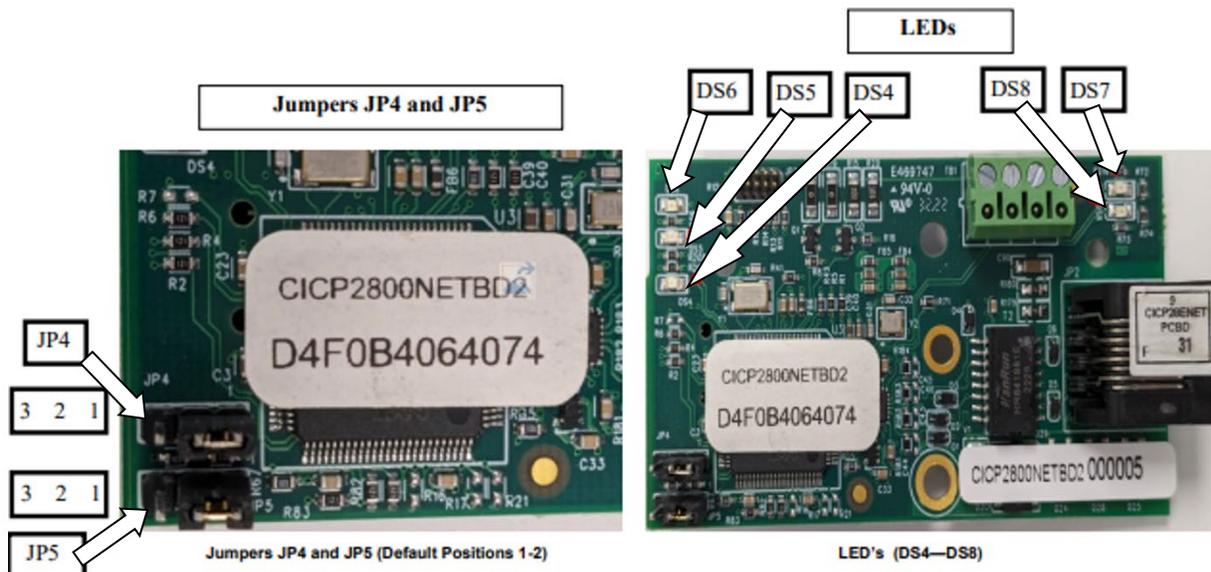
JP5 (Reset Universe Finder Utility Username and Password)

The following procedure is used reset the Web utility Username and Password back to the default of "admin" and "admin".

1. Move Jumper JP5 to positions 2-3.
2. Cycle power to Accelterm.
3. Wait 30 Seconds, the Green/Red LEDs stop flashing
4. Then Restore Jumper JP4 to positions 1-2.
5. Restore Jumper JP5 to positions 1-2.
6. The Universe Finder Username and Password is reset to "admin" and "admin".

Jumper Settings	
Jumper	Function
JP4	1-2 Normal Location (as shown)
	2-3 Used to clear the current IP address information and configure for DHCP
JP5	1-2 Normal Location (as shown)
	2-3 Used to Reset Universe Finder utility Username and Password to "admin" and "admin"

LED Functions	
LED	Function
DS4	Fast Blink = Firmware is in bootloader Slow Blink = Application is running Off/On = Micro is not running
DS5	Fast Blink = Firmware is in bootloader Solid On = DHCP is searching for IP Off = IP address obtained
DS6	On = Static IP Configured Off = Static IP Not Configured
DS7	On = Ethernet Connected Fast Blink = Ethernet is communicating
DS8	10/100 Link Operating Speed Indication ON = 100Mbps OFF = 10Mbps



APPENDIX C – Reset Procedure for uniVerse CICP2100 (Single Door Double Gang Model)

Note: You will need a jumper to complete the reset step below

J3 (Configure for DHCP Request)

The following procedure is used to clear the current IP address information and configure for DHCP (see table 19).

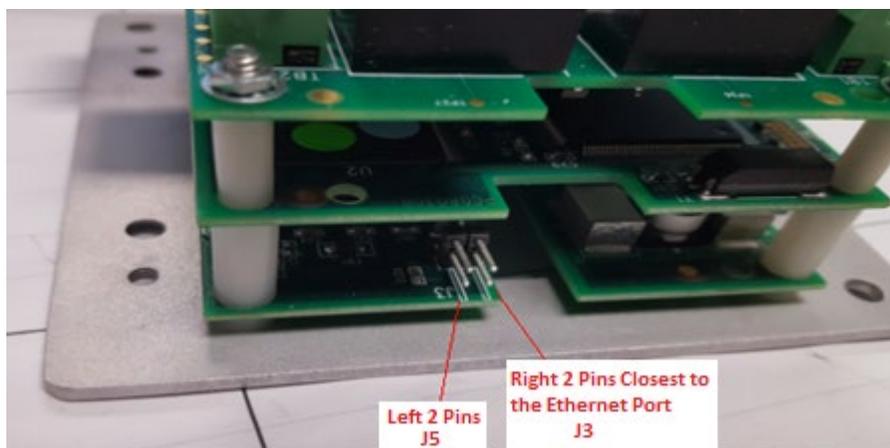
1. Install Jumper J3 (IN).
2. Cycle power to uniVerse®.
3. Remove Jumper J3.
4. The uniVerse® should obtain a new IP address from DHCP.

J5 (Reset Web Utility Username and Password)

The following procedure is used to reset the Web utility Username and Password back to the default of "admin" and "admin".

1. Install Jumper J5 (IN).
2. Cycle power to uniVerse®.
3. Remove Jumper J5.
4. The Web Utility Username and Password is reset to "admin" and "admin".

Jumper	Function
J3	Out = Default IN = Default to DHCP
J5	OUT = Default IN = Reset Web Username and Password to "admin" and "admin"



APPENDIX D – Reset Procedure for uniVerse CICP2100S (Single Door, Surface Mounted Enclosure Models)

New Single Board Model

JP9 (Configure for DHCP Request)

The following procedure is used to clear the current IP address information and configure for DHCP (see table 19).

1. Before power cycle move Jumper JP9 to Pin 1-2
2. Cycle power to the uniVerse®.
3. Move Jumper JP9 back to normal operation Pin 2-3
4. The uniVerse® should obtain a new IP address from DHCP.

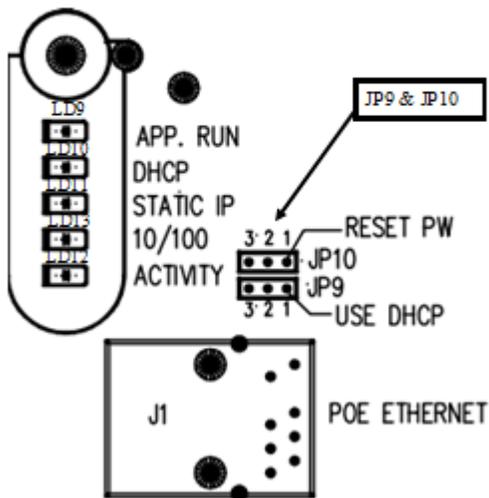
JP10 (Reset Web Utility Username and Password)

The following procedure is used reset the Web utility Username and Password back to the default of "admin" and "admin".

1. Before power cycle move Jumper JP10 to Pin 1-2
2. Cycle power to the uniVerse®.
3. Move Jumper JP10 back to normal operation Pin 2-3
4. The Web Utility Username and Password is reset to "admin" and "admin".

Note: The JP9 and JP10 jumpers are located on top of the ethernet port

Jumper	Function
JP9	Pin 2-3 = Normal Operation Pin 1-2 = Default to DHCP
JP10	Pin 2-3 = Normal Operation Pin 1-2 = Reset Web Username and Password to "admin" and "admin"



Legacy 4 Board Model

J3 (Configure for DHCP Request)

The following procedure is used to clear the current IP address information and configure for DHCP (see table 19).

1. Install Jumper J3 (IN).
2. Cycle power to uniVerse®.
3. Remove Jumper J3.
4. The uniVerse® should obtain a new IP address from DHCP.

J5 (Reset Web Utility Username and Password)

The following procedure is used reset the Web utility Username and Password back to the default of "admin" and "admin".

1. Install Jumper J5 (IN).
2. Cycle power to uniVerse®.
3. Remove Jumper J5.
4. The Web Utility Username and Password is reset to "admin" and "admin".

Note: The J3 and J5 jumpers can be easily accessed through the knockout for the Ethernet cable.

Jumper	Function
J3	Out = Default IN = Default to DHCP (2 pins closest to ethernet cable slot)
J5	OUT = Default IN = Reset Web Username and Password to "admin" and "admin"

