DB-04 CC501
Wireless Bridge
&
DB-02 D-link DAP-2553
Access Point

Installation and Operation Manual

Limited Warranty

Cirus Controls, LLC.

What and who is covered?

This warranty covers all defects in materials or workmanship in your Cirus Controls system under normal use, maintenance and service. This warranty coverage applies only to the original owner and is not transferable.

How long is the warranty period?

This warranty coverage runs for a period of 1 year from the date of initial installation (or 13 months from date of shipment from Cirus Controls), whichever occurs first. Replacement parts are warranted for the remaining portion of the original warranty period or thirty (30) days from date of shipment from our factory (whichever is greater).

How can you get service?

Cirus Controls' obligation under this warranty is limited to repairing and/or replacing, at Cirus Controls' option, any part or parts that are determined, by Cirus Controls, to be defective. To be eligible for any claim under this warranty, the owner (or Cirus authorized dealer) must return any defective part(s) to the factory, within the applicable warranty period (as set out above).

What will we do?

Cirus Controls' may, at its option, elect to grant adjustments in the field through an authorized representative and may thereby elect to waive the requirement that parts be returned to Cirus Controls' factory. The repair or replacement of defective parts under this warranty will be made without charge to the owner except for transportation of the part to our authorized repair location.

What is not covered under this warranty?

Cirus Controls will not assume any expense or liability for repairs made outside our plant without our prior written consent. We are not responsible for damage to any associated equipment or product and will not be liable for loss of profit or other special damages.

The provisions of this warranty do not apply to any product or parts which have been subject to misuse, negligence or accident, or which have been repaired or altered outside of Cirus Controls' factory in any way (in the judgment of Cirus Controls) so as to affect adversely its performance or reliability. Neither does this warranty apply to normal maintenance service and parts or to normal deterioration due to wear and exposure.

This warranty is expressly in lieu of other warranties, expressed or implied, in fact or by law, including any implied warranty of merchantability of fitness for a particular purpose. The remedies of repair or replacement as set forth are the only remedies under this warranty, Cirus Controls' disclaims any obligations or liability for loss of time, inconvenience, commercial loss or direct consequential, special or incidental damages. This warranty is in lieu of any other obligation or liability of Cirus Controls' of any nature whatsoever by reason of the manufacture, sale, lease or use of such products and Cirus Controls neither assumes, not authorizes anyone to assume for it, any other obligation or liability in connection with such products.

Revision Level of this Manual

Rev Letter	Effective Date	Contents
A	8-1-10	Initial Release of Wireless Manual
B	10-28-11	Change to CC501 Bridge
C	11-30-11	General Update
D	3-24-12	Bridge default IP change to 192.168.103.2
E	9-12-12	DAP-2553 instructions added
F	1-29-13	General update

Cirus Controls reserves the right to make changes to this manual from time to time without notice.

> *Note: this manual includes both wireless devices that are required for a functional* ***Drive by Download*** ***TM*** *system. Your package will only include what was ordered, thus may or may not include the below DB-04/DB-02 contents.*

DB-04 Package Contents

DB-04 Wireless Ethernet Bridge includes the following items:
1.) One Airborne Direct™ Ethernet Bridge with an attached 6’ RJ-45 plug.
2.) One TS-3001 power adapter.
3.) One mounting cradle with Velcro
4.) One Quatech CD containing documentation and software, the AMC utility or web browser is required for modification of the programmed unit.
5.) 512-MB or 1-GB Secure Digital (SD) or MMC memory card (if ordered with ***SpreadSmart****TM* or ***Datashark****TM* the card is already installed.)

DB-02 Package Contents

DB-02 Wireless Access Point includes the following items:
1.) One DWL-2100AP Access Point
2.) One 120Vac Power adapter
3.) One Ethernet cable.

Unpack the wireless devices that were ordered and compare the contents with the items listed above. If any of these items are missing, please contact your distributor and/or dealer for replacement parts.

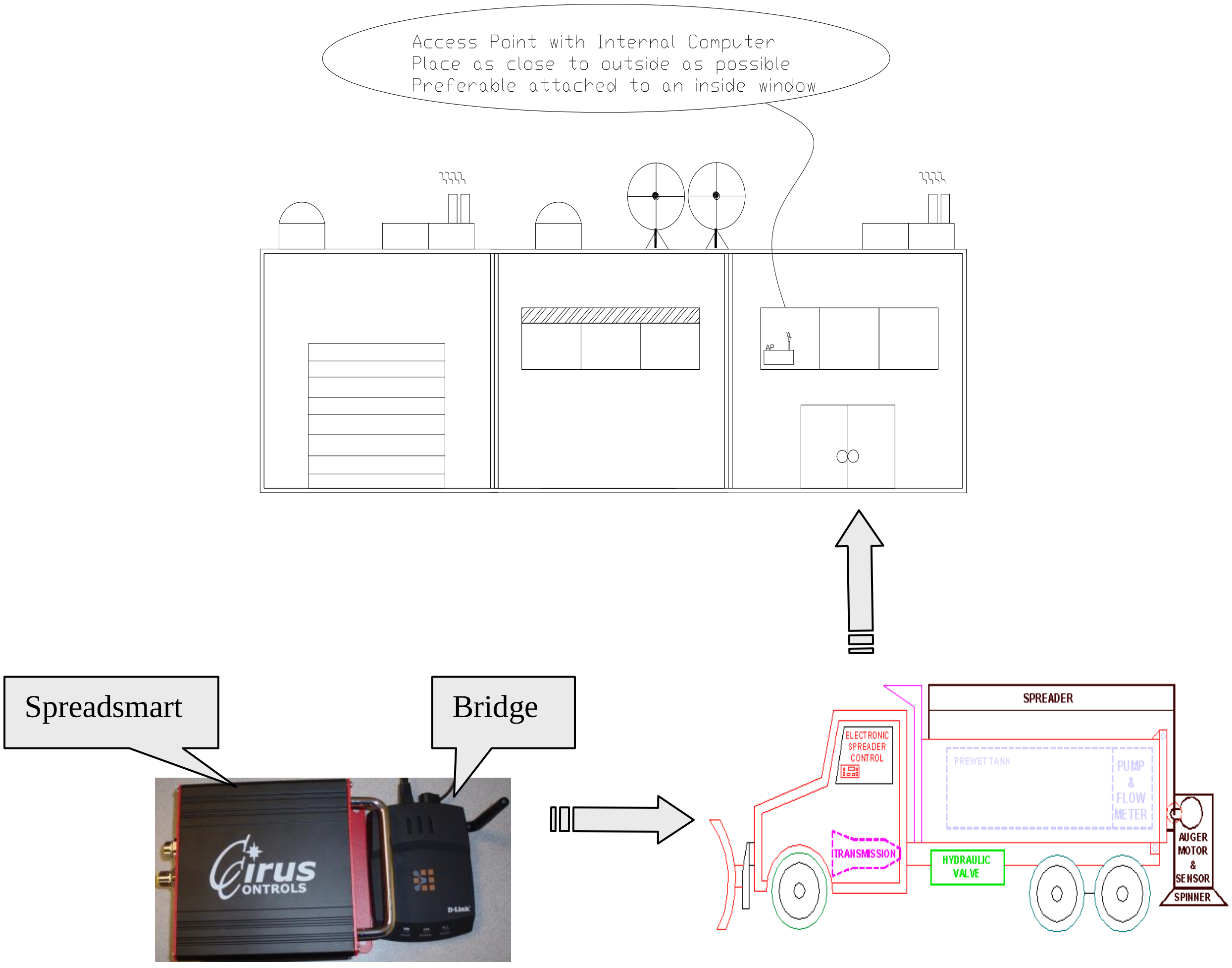
Support

If you have any questions about your ***Drive by Download*** ***TM*** system or it’s operation call the Cirus Controls Technical Support line at: (763) 493-9380. Technical Support is available Monday thru Friday from 7am to 5:00pm central time. You may also e-mail customer support with your questions at info@ciruscontrols.com.

Functional Overview

Drive by Download ***TM*** is a wireless data transfer device that uses WiFi technology to transfer stored data from a truck (mobile) data storage device to a base station computer. ***Drive by Download*** ***TM*** is compatible with ***SpreadSmart******TM*** and ***Datashark******TM*** systems. The CC501 & 2100AP is shipped from Cirus Controls ready to use. Should you need to change any of the preconfigured settings, refer to the "configuration section".

Signal Flow Chart of Recording Device


Access Point with Internal Computer
Place as close to outside as possible
Preferable attached to an inside window
AP
Spreadsmart
Bridge
Cirus CONTROLS
D-Link
SPREADER
ELECTRONIC SPREADER CONTROL
PREWET TANK
PUMP & FLOW METER
TRANSMISSION
HYDRAULIC VALVE
AUGER MOTOR & SENSOR
SPINNER

What Is Required for a Functional System

To complete your installation you need:
1.) An Ethernet client (i.e. ***SpreadSmart^{TM} or Datashark^{TM}***). The Ethernet client must be within the Transmit and Receive range of the Access Point (DB-02) which will link with the DB-04 (bridge).
2.) A computer with an internal network-interface card (NIC).
3.) ***Drive by Download^{TM}*** Software Suite.
4.) A DB-04 Wireless Bridge
5.) A DB-02 Wireless Access Point

Pre-Delivery

Step 1 - Wireless Ethernet Bridge Install

The hardware installation on the truck side consists of installing and connecting the wireless bridge and installing the Secure Digital card (SD) into the ***SpreadSmart^{TM}*** or ***Datashark^{TM}*** system.

NOTE: If the system was ordered with a DB-04 (bridge), the SD card will already be installed, skip step 2.

The wireless bridge should be mounted on the back wall of the cab, or on the dashboard. In either case, the wireless bridge <u>must</u> be installed in a protected location where the antenna is visible through the windshield. Choose the location with cable length in mind with relationship to the data collection device. Do not permanently mount the wireless bridge until data transfer from truck to base station is validated (step 3-4).

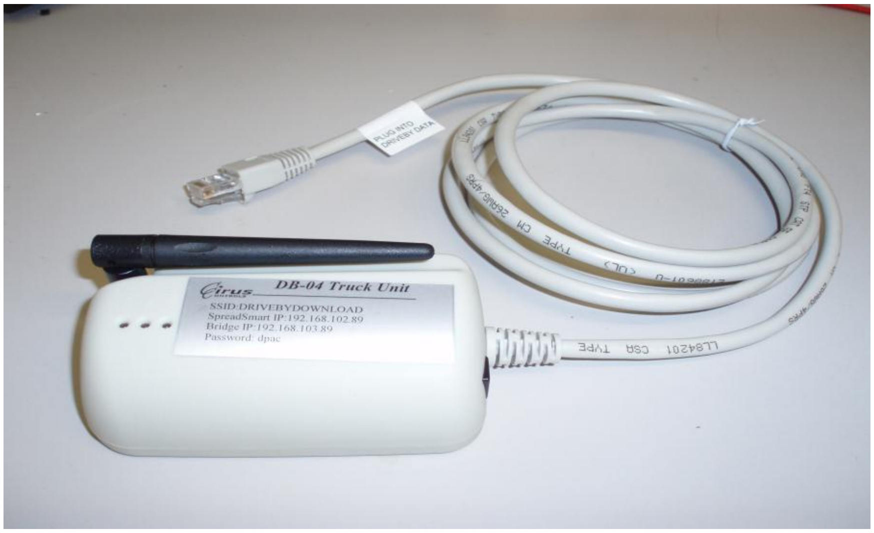


Figure 1.0

Connecting the Bridge to the *SpreadSmart^{TM}* or *Datashark^{TM}*.

1.) Connect the power adapter to the back panel on the wireless bridge (figure 1.0) plug the other end of the power adapter into the ***SpreadSmart***^{TM} ***or Datashark***^{TM} end plate labeled Aux Power (figure 1.1).

2.) Install the male end of the 6' Ethernet RJ-45 cable into the **`Drive By`** port (figure 2.0).

3.) Power up the ***SpreadSmart***^{TM} or ***Datashark***^{TM}, verify that the power led lights on the wireless bridge (wait about 10-40 seconds)

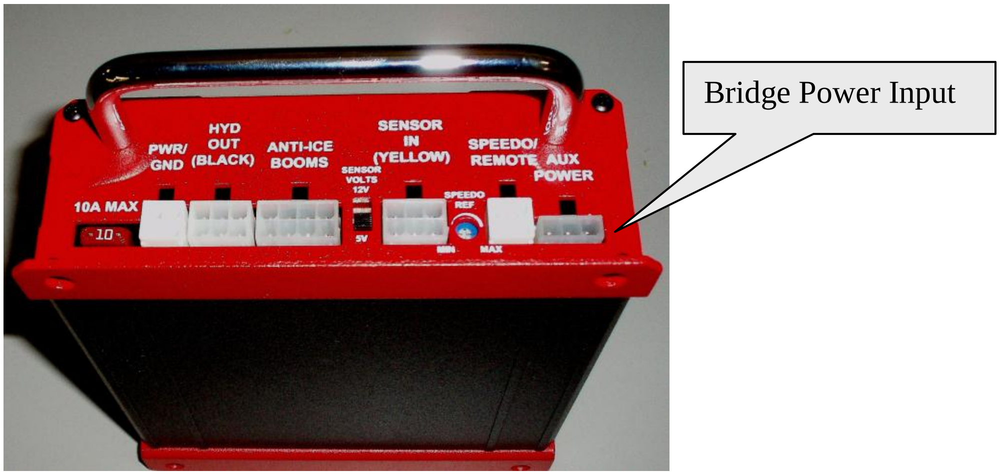


Figure 1.1

Step 2 – Installation/Removal of SD (Digital Storage) Card

Shut off the power and remove the 4 screws on the access plate that has the **`Drive By Data`** port (figure 2.0). Grasp the opposite end plate by the silver handle and carefully slide out the PC board. **HANDLE THE CIRCUIT BOARD WITH CARE!**

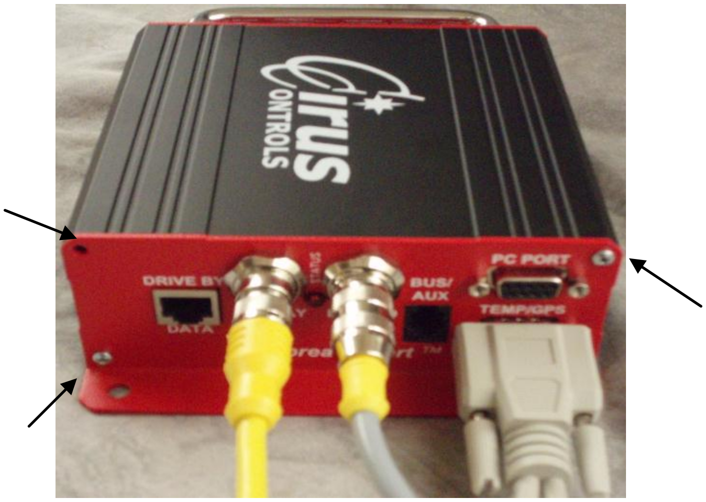


Figure 2.0

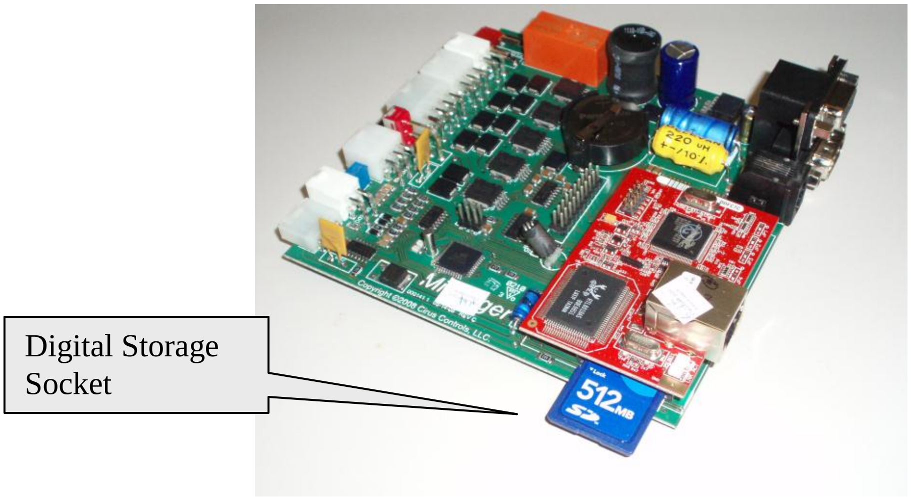


Figure 2.1

Installation

1.) Locate the Rabbit core, this is located on the end of the circuit board, it is the side that has the Ethernet jack. The SD card socket is beneath the core and can be seen from the edge of the circuit board (Figure 2.1)

2.) Make sure the "Locked" tab on the SD card is not in the locked position. Next, with the gold tabs facing downward (figure 2.1) gently slide in the SD card into the socket. *Note: Make sure that the card latched into its mating socket.*

3.) Slide the circuit board into the case and re-install the 4 self-tapping screws.

4.) Mount the enclosure back in the vehicle.

5.) Connect all previously attached cables (keypad, LCD, hydraulic, sensor and power cables).

6.) Insert the RJ-45 plug on the bridge into the `Drive By Data` port (figure 2.2). Make sure the cable latches/clicks to prevent intermittent connections.

Removal

To remove reverse the installation steps.

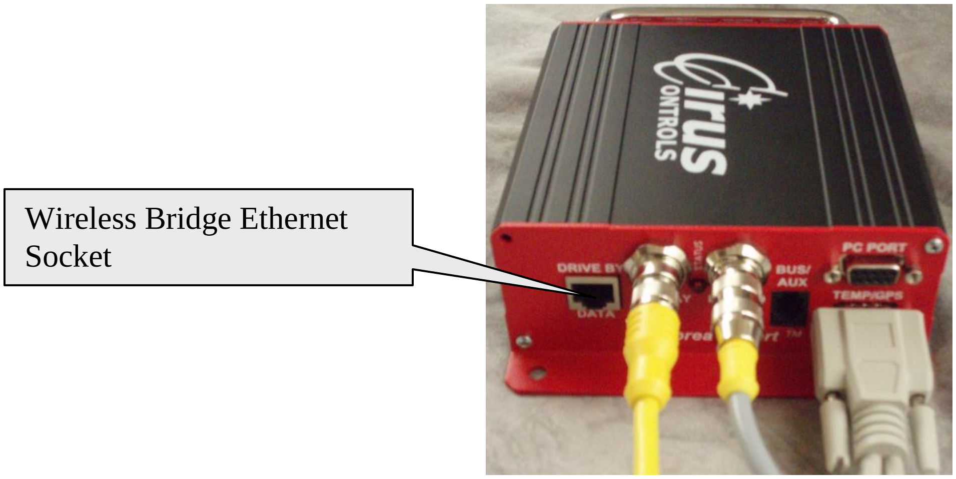


Figure 2.2

Next, power up the ***SpreadSmart***^{TM} or ***Datashark***^{TM} system. Verify that the power LED on the bridge is fixed and lights continuously. The Link light will be solid when there is an AP within range and the Comm. light will flash "On" and "Off" (this is normal operation).

Step 3 - DB-02 (Access Point) Hardware Installation

The hardware installation on the computer side consists of connecting the DB-02 “Access Point” to a computer, existing network hub, switch, or router and connecting the Ethernet and power plug into the back of the access point.

Determine the location to mount the access point: the Access Point is best mounted in a location where it has an unobstructed line of sight with all trucks during normal operations (fueling, loading salt, etc). This can be in an office window, parking garage, etc. Although testing has shown success with putting the access point inside an office/garage with no line of sight access to the vehicles, the range of wireless communication is severely limited by such a location. After installation, if it is determined that the range of communication is unacceptable, relocating the access point will often aid in increasing the range. Normal operating range is 250 feet (with clear line of sight mounting), however, testing has shown ranges in excess of 500 feet with ideal conditions.

Connecting the cables to the access point

1.) Connect the barrel adapter into the back of the AP (access point) followed by the other end into a wall 120Vac outlet.
2.) Plug in one end of the Ethernet cable into the Ethernet port on the back panel of the access point and the other end of the cable into your network (switch, router or computer).
3.) When both cables are connected and a link is established, the Power and LAN LED will light on the access point.

Step 4 - Base Station Computer Configuration

Network Description

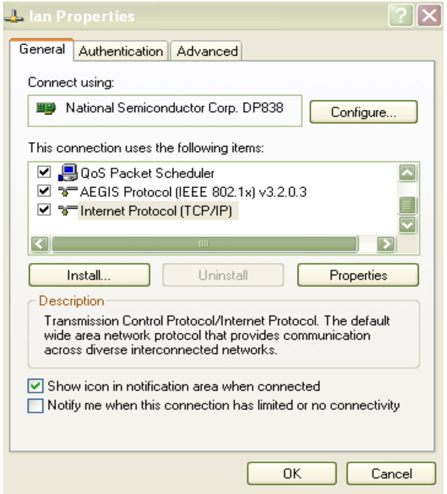
All of the ***Drive by Download*** ***TM*** components (bridge and access points) must have unique IP address’s and be within the same subnet. Components are configured at the factory to operate in the 192.168.(98-111).(1-254) range. Most network configurations allow for transparent communication between the ***Drive by Download*** ***TM*** components without changes, however, in the event of a conflict with an existing network, the TCP/IP settings on all the components can be modified to operate in a different subnet. A silver sticker placed on the bridge and access point indicates the IP address, SSID and password.

NOTE: IP address modification should only be done by a qualified computer technician that has a complete understanding of TCP/IP networking concepts with experience setting up wireless networking components. All components of the ***Drive by Download******TM*** system must be located in the same subnet for everything to function correctly.

Setup when access point connected directly to a computer or to a LAN using the same subnet (Typical Setup-XP instructions):

1. Select **Start**
2. Select **Control Panel**
3. Click on **Network Connections**
4. Click on the **Local Area Network** icon
5. Select **Properties**
6. Double-click the **Internet Protocol (TCP/IP)** line (figure 3.0)
7. Select **Use the following IP address** and enter in an IP address in the 192.168.96.1 through 254 range. **NOTE:** This number cannot be the same as the access point or any bridge. Use 255.255.240.0 for the subnet (figure 3.1) click **OK** twice to close out the Internet Protocol/LAN properties. The computer is now ready to send/receive data via from the access point.
8. Open your web browser and type the IP address that is located on the silver sticker on top of the access point into the address bar and press **ENTER**. The access point login screen should appear. If this is not the case, verify steps 1-7

Note: *step 7 is important verify this before proceeding.*



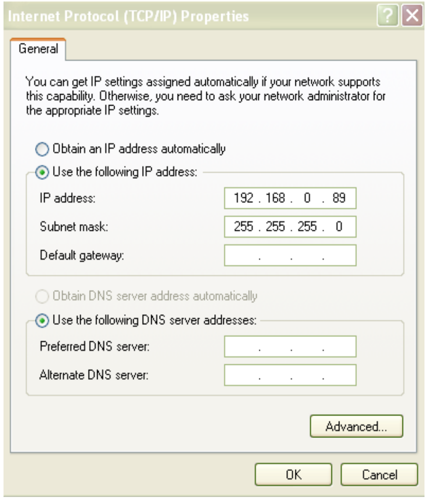
Connect using:
National Semiconductor Corp. DP838

This connection uses the following items:
☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.2.0.3
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☐ Notify me when this connection has limited or no connectivity

Figure 3.0



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 89
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

Figure 3.1

Setup when access point is connected to a switch, router or hub where the *Drive by Download*^{TM} network and LAN are on different subnets: (XP Instructions)

NOTE: the local network administrator will need to supply information for this type of setup.

1.) Power up the computer that will be used for the ***Drive by Download*** ^{TM} system.
2.) Select **Start**
3.) Select **Control Panel**
4.) Click on **Network Connections**
5.) Click on the **Local Area Network** icon
6.) Select **Properties**
7.) Double-click the **Internet Protocol (TCP/IP)** line (figure 3.0)
8.) If **Obtain an IP address automatically** (DHCP) is checked (figure 3.1) you will need to get an open static IP address, subnet mask value, default gateway value and DNS server values before proceeding. Contact your local network administrator.
9.) When the computer is set up with a static IP address and the DNS server values are present, verify that the Internet works (if the Internet is available). *If it does proceed to step 10, if not verify settings, this needs to work before proceeding.*
10.) Select **Advanced**
11.) Select **Add** on the IP settings tab and enter a unique address (i.e.192.168.96.1 through 192.168.96.254.)
12.) Enter the subnet value 255.255.240.0.
13.) Click **Add** then **OK** to close the advanced settings. Click **OK** twice to close the Internet Protocol and LAN properties dialog boxes.
14.) Open your web browser and type the IP address that is located on the silver sticker on top of the access point into the address bar and press **ENTER**. The access point login screen should appear. If this is not the case, verify steps 2-12

You should now be ready to access the full Wi-Fi power of your ***Drive by Download*** ^{TM} system. Refer to the ***Drive by Download*** ^{TM} "***Utility & Data Analysis***" manual to complete the setup & download of each truck in your fleet.

Troubleshooting Suggestions

The Bridge cannot find the Access Point.	Verify that the **Link** LED is solid green. If it isn't, refer to "LED Troubleshooting" in the Quatech manual located on the Quatech CD.
The Access Point does not communicate with the computer.	Make sure Power is applied to the Access Point Make sure that the AP is connected to your network or computer via the Ethernet cable Verify that Leds on the unit are green and are blinking. If the problem remains, reset the unit and reconfigure.
You cannot access the Bridge's configuration interface via the AMC.	You may have typed the wrong static subnet address. Check computers IP and subnet. Be sure the computer and Bridge are on the same subnet of the same network.
The Bridge cannot associate with an Access Point.	Change the location of the Bridge to improve reception. If that does not help, launch the AMC, go to the Network Settings Page, and be sure the SSID & encryption matches that of the Access Point (remember the SSID is case sensitive). Check encryption
You used the AMC to change the Bridge's configuration settings, but the new settings did not take effect.	You may not have clicked the **Save** button on the AMC page. Click this button after making your changes on the page.
After changing the Bridge's static IP address, the AMC stops responding.	Once the static IP address is changed and you click **Save**, the Bridge switches to the new IP address and loses connection with the AMC. To resolve this problem, restart the AMC-make sure your on the same subnet.
The Access Point doesn't take the settings when set with the wizard	Manually configure the Access Point by not going thru the wizard.

Resetting the Bridge or Access point:

CAUTION

CAUTION: doing this will set the unit back to factory settings (this is not recommended, verify all previous steps before proceeding)

1.) Reset Access Point (DB-02) or Bridge (DB-04):

A) Hold down the reset button (restore) on the back of unit for 15 seconds (will need small paperclip or needle.)

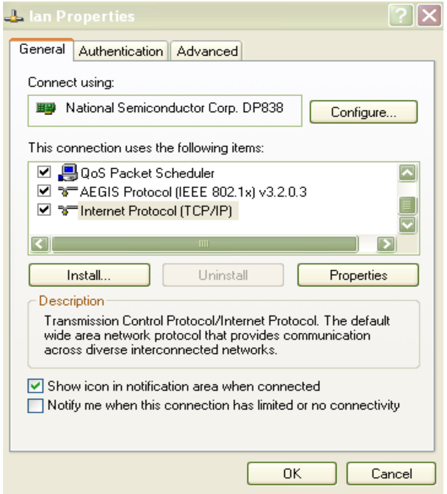
B) Power up the Access Point or Bridge

C) Verify the LEDs on the front of unit turned off and then back on

D) Release the reset button and power cycle the device. Hold the reset button down again for 15 seconds (DB-02 only).

Configuring the computer to talk to the Bridge/Access Point:

1.) Select **Start**
2.) Select **Control Panel**
3.) Click on **Network Connections**
4.) Click on the **Local Area Network** icon
5.) Select **Properties**
6.) Double-click the **Internet Protocol (TCP/IP)** line (figure 4.0)
7.) Select **Use the following IP address** and enter in an IP address 192.168.0.51 (figure 4.1) for the DWL-2100AP or 192.168.103.3 for the CC501.
8.) Click **OK** twice to close out the Internet protocol/LAN properties. The computer is now ready to communicate with a factory default bridge or access point.



lan Properties

General | Authentication | Advanced

Connect using:

National Semiconductor Corp. DP838 [Configure...]

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.2.0.3
☑ Internet Protocol (TCP/IP)

[Install...] [Uninstall] [Properties]

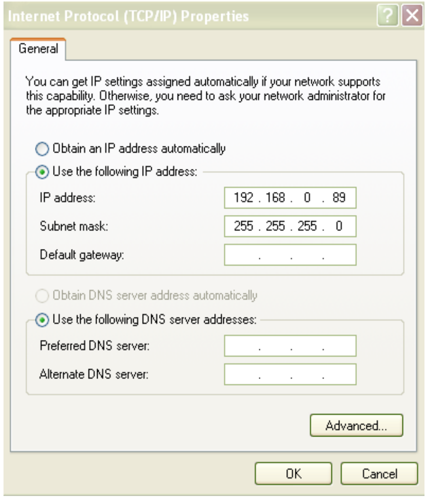
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☐ Notify me when this connection has limited or no connectivity

[OK] [Cancel]

Figure 4.0



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 89
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

[Advanced...]

[OK] [Cancel]

Figure 4.1

Configuring the Bridge using the Airborne Management Center (AMC)

Install the Quatech CD-only if the AMC utility is <u>not installed</u> on the computer you're using. ***Note: if the DataManagement Suite is > 3.8 this will be located in C:\Program Files\Cirus Controls\Data Management Suite\Quatech Bridge***

Note: *The AirborneDirect Wireless Ethernet Bridge can be configured by wireless connection, however, <u>only</u> if you have wireless access from associated computer. To do this setup your computer to be within the same IP subnet as the bridge, followed by opening the AMC utility.*

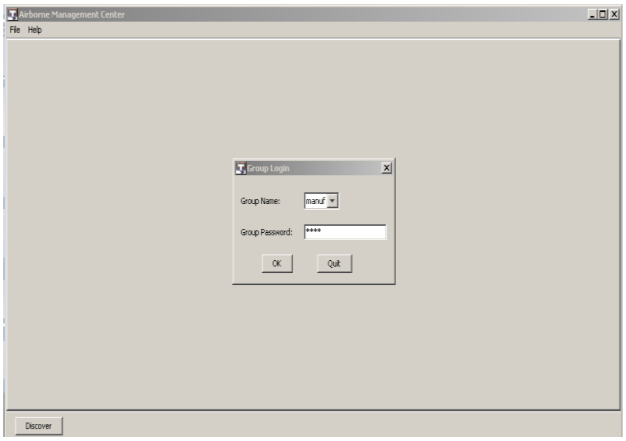
*Complete "**Configuring the computer to talk to the Bridge/Access Point"** section before proceeding*

Programming the Quatech Bridge CC501

a. Set an IP address into the computer from the "***Configuring the computer to talk to the Bridge/Access Point pg.13***" section and disable the computer internal wireless card.

b. Open the Airborne Management Center Icon under programs.

c. Group logon will come up type in "dpac" for the Group Password

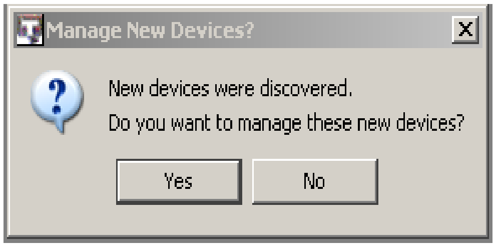


Group Name: manuf

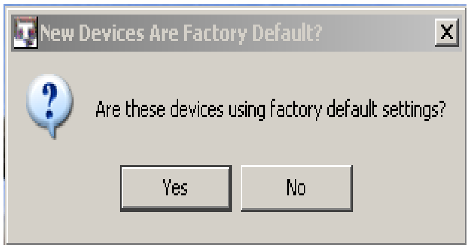
Group Password: ****

d. Click "yes" to manage these new devices

e. Click "yes" for these systems are using factory default settings



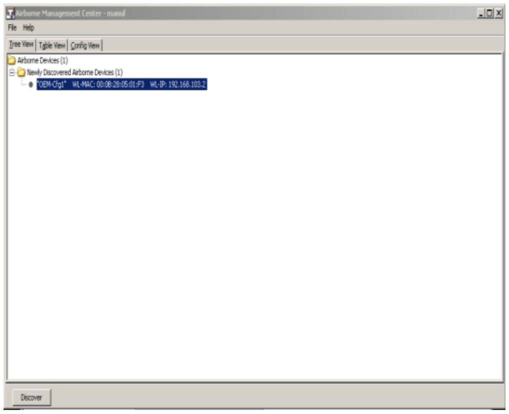
New devices were discovered.
Do you want to manage these new devices?



Are these devices using factory default settings?

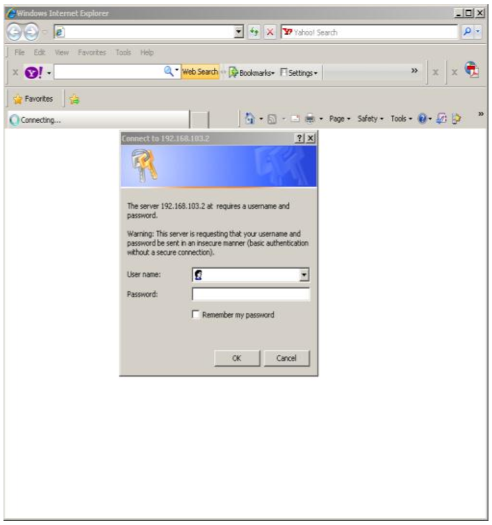
f. Under the tree view you should see an IP address of 192.168.103.2. This is the default IP address for the CC501 bridge. **Right click** on OEM-cfg-1, followed by **connectivity tools->launch web browser**

NOTE: If the system does not show your device, make sure it is powered up and verify the steps in "Configuring the computer to talk to the Bridge/Access Point" section.



Airborne Devices (1)
Newly Discovered Airborne Devices (1)
"OEM-Cfg1" WL-MAC: 00:0B:28:05:01:F3 WL-IP: 192.168.103.2

g. Type “**dpac**” for username and password



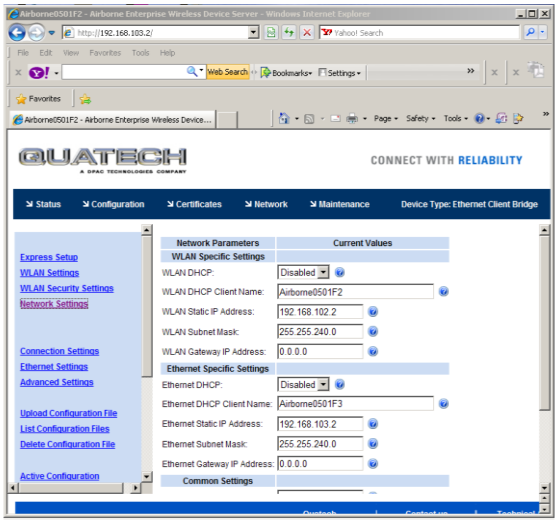
The server 192.168.103.2 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

□ Remember my password



Network Parameters	Current Values
WLAN Specific Settings	
WLAN DHCP:	Disabled
WLAN DHCP Client Name:	Airborne0501F2
WLAN Static IP Address:	192.168.102.2
WLAN Subnet Mask:	255.255.240.0
WLAN Gateway IP Address:	0.0.0.0
Ethernet Specific Settings	
Ethernet DHCP:	Disabled
Ethernet DHCP Client Name:	Airborne0501F3
Ethernet Static IP Address:	192.168.103.2
Ethernet Subnet Mask:	255.255.240.0
Ethernet Gateway IP Address:	0.0.0.0
Common Settings	

h. Click on “Express Setup”. Change the SSID to “**DRIVEBYDOWNLOAD**”

i. Select WLAN security type to “**Enabled**”. Cirus default encryption is **Wep 64-key 1** is “**8B0EA37480**”, this will not be seen when the screen is loaded, however, if the 2 led’s on the bride are green there is no need to enter it.

j. Set **WLAN DHCP** & **Ethernet DHCP** to “disabled”

k. Set the **WLAN IP address** to the same as the ***SpreadSmart***^{TM} or ***Datashark***^{TM} IP address

l. Set the **Ethernet static IP address** to the bridge (DB-04) IP address; located on the silver sticker.

m. Set the **WLAN and Ethernet subnet** to 255.255.240.0

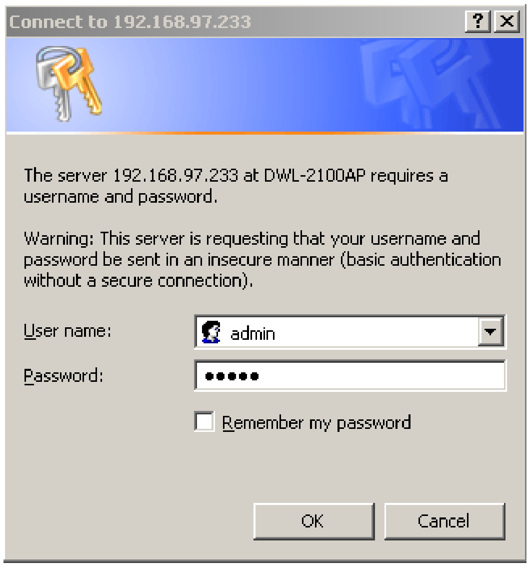
n. Change the Telnet port to 9023. Press commit & restart

o. Configuration is now completed

> ***NOTE***: *determine whether the Bridge IP address changed. To confirm that the settings took place you will need to set your computer to be in the same subnet as what was just programmed into the device & rescan for that IP address.*

Configuring the DB-02 Access Point D-link DAP-2553

1. Connect the power adapter to the receptacle on the back panel, and then plug the other end of the power adapter to a wall outlet (120Vac) or power strip.
2. Insert in one end of the Ethernet cable into the Ethernet port on the back panel of the access point, and the other end of the cable into your computer.
3. Set computer to talk to the access point in the “**Configuring the computer to talk to the Bridge/Access Point section pg 13**” *use IP address 192.168.0.51.*
4. Open your web browser and type http://192.168.0.50 for the DWL-2100AP. Press **ENTER** to connect.


Connect to 192.168.97.233

The server 192.168.97.233 at DWL-2100AP requires a username and password.

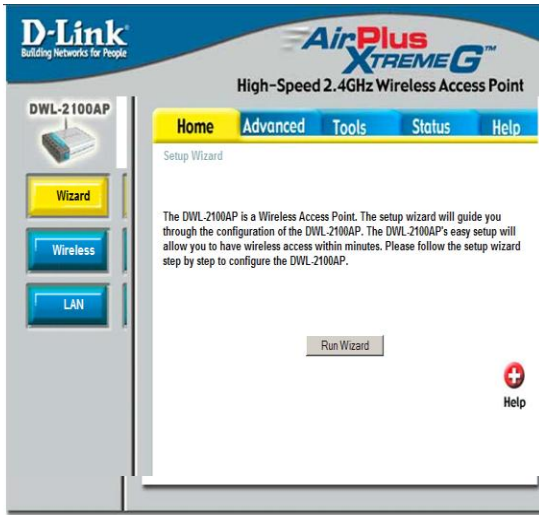
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

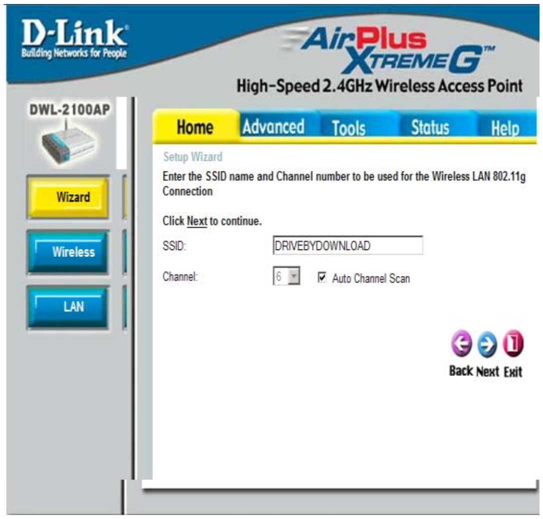
Password: ●●●●●

□ Remember my password

5. Log in using lowercase **admin** for username and leave the password field blank. Click **OK.**



The DWL-2100AP is a Wireless Access Point. The setup wizard will guide you through the configuration of the DWL-2100AP. The DWL-2100AP's easy setup will allow you to have wireless access within minutes. Please follow the setup wizard step by step to configure the DWL-2100AP.



Enter the SSID name and Channel number to be used for the Wireless LAN 802.11g Connection

Click Next to continue.

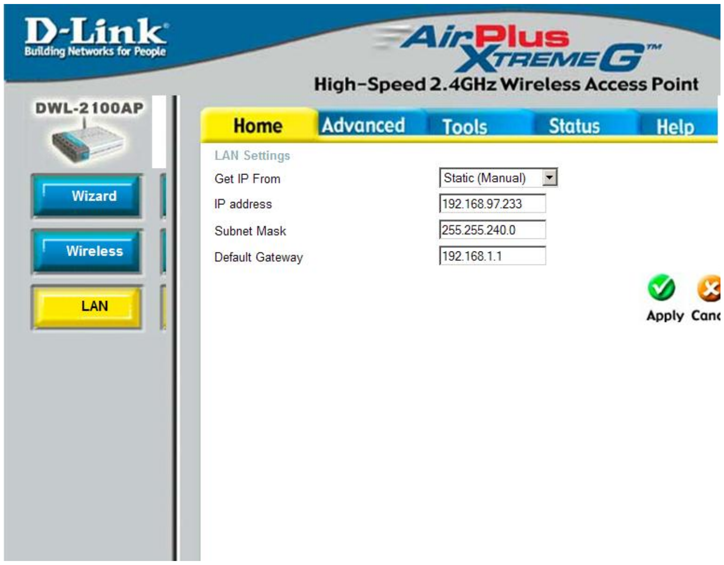
SSID: DRIVEBYDOWNLOAD

Channel: 6 ☑ Auto Channel Scan

6. From the D-Link home page, click on Tools. Add the new & conformation password to *"CIRUS"*.
7. Retype in the username (admin) and password (CIRUS) this will bring you back to the home page.
8. Click on the "**Wireless**" tab, set the **SSID to "DRIVEBYDOWNLOAD**"
9. Enable the encryption to **WEP 64**, type in key 1 as "**8B0EA37480**", leave all other keys blank, verify that your typing is correct. Press OK and recycle the system.

Note: if the encryption has been changed in your facility this will need to be known. One mistyped character will prevent the system from working.

9. Retype in the username (admin) and password (CIRUS) this will bring you back to the home page.



LAN Settings

Get IP From: Static (Manual)

IP address: 192.168.97.233

Subnet Mask: 255.255.240.0

Default Gateway: 192.168.1.1

10. You should now be on the Dlink home page. Click on **LAN**
11. Type in the **IP address** that is on the access point (**silver sticker**) or set it to an open IP address from your IT administrator.
12. Make sure the **subnet** is set to 255.255.240.0; set the **gateway** to 192.168.96.1. Click on Apply followed by continue. The main page should now be present.

Configuration is now complete.

Useful Terms to Know

You'll find these network terms throughout this manual. As an installer of Cirus Controls ***Drive by Download*** *TM* systems, a simple explanation of "all those numbers" and what they mean is a useful tool while setting up systems. As such this guide is not designed to give the reader a complete understanding of all the systems and protocols associated with Internet Protocol networking, just a basic understanding of the settings affected by installing a ***Drive by Download*** *TM* system.

IP Address

The Internet is a collection of individual networks tied together. Each of these smaller networks is called a subnet (more on this later). Inside each subnet, all networked components (computers, bridges, spreader units, etc) have an address that differentiates those components from each other. It is required that all networked components inside a subnet have a **unique** address. This allows the other components in that subnet to identify who is "talking". The address is typically expressed as a **dotted quad** address. It looks like four numbers from 0 to 255 separated by periods. An example would be 172.154.23.58. The addresses of a subnet must be similar to each other if the components are to communicate with each other.

Subnet

This is usually the most difficult part of the system to grasp. Some of the concepts here are simplified to allow the non-technical user to understand these concepts, and should not be accepted as concrete rules. Advanced IT personnel will note that technologies such as advanced routing and tunneling can be used to break these rules, but that is not germane to this discussion.

As mentioned previously, the Internet is made up of a collection of individual networks that are tied together. These individual networks are called subnets. The way messages get passed between computers inside the same subnet and computers on different subnets is different. If one component is communicating with another component on the same subnet, the communication is “broadcast”. This means that all the network components on the subnet can hear the communication. The message envelope determines the “addressee”. If a component on a subnet hears a communication that is not addressed to it, it just ignores the message and moves on. If the communication is addressed to that component, it is received and processed.

When two components communicate and they are on different subnets, the communication is “routed”. Each subnet (which is “routable”) has a gateway. The gateways job is to take messages destined for components outside of it’s own subnet and hand them off to the “upstream” message handler, who then determines what to do with it. Gateways are commonly referred to as “routers”.

When a component generates a message, it determines if it’s bound for a component inside its own subnet, or a component outside the subnet. If the component is inside the subnet, the message is broadcast, if the component is outside the subnet, it’s handed off to the gateway to pass to another subnet. The way each component determines if another component is in its own subnet or on a different subnet, is by using something called a subnet mask. The subnet mask is also a dotted quad number. While the subnet mask numbers can contain numbers different than 255 and 0, this requires an understanding of binary masking and is beyond the scope of this primer.

Let’s assume that a subnet mask is 255.255.0.0. If a component looks at the destination components address, and “masks” the numbers that are represented in the mask by a 0, and compares the remaining numbers, the remaining numbers must match to be in the same subnet. So if the sender’s address is 172.57.43.27 and the recipient’s address is 172.57.32.89, the mask is applied to the recipient’s address, and 172.57.x.x results. Since those two numbers are the same as the senders address numbers, the recipient is in the same subnet. If the senders address is 172.57.43.27 and the recipient is 10.23.45.67, the recipients address (after being masked) is 10.23.x.x. Those numbers do not match and the recipient is on a different subnet. This communication would be handed off to the gateway and routed appropriately.

A final point. There are physical subnets, and numerical subnets. A physical subnet is a group of components that is physically tied together without traveling through a router.

(Note some routers have hubs/switches built in which confuses this subject. On these types of routers, there are what's called a LAN ports and a WAN port. The LAN ports tie to the same subnet; the WAN port is the link to other subnets). One physical subnet can have multiple numerical subnets that can run simultaneously without interfering with each other. However, numerical subnets MUST exist on the same physical subnet.

For example: We have a hub with four computers tied to it. Their addresses and subnet masks define two of these computers as being in one numerical subnet. The other two are defined by their addresses and subnet masks as being in another numerical subnet. The first two computers can communicate with each other, and the last two computers can communicate with each other, but computers from the first group cannot communicate with computers from the last group. Even though they are on the same physical subnet, there is no method for them to communicate with each other.

Gateway

The gateway was discussed in the previous section. Its function is to pass messages from its own subnet to other subnets. In order for it to receive messages from its own subnet, its address must fall into the numerical subnet it is passing messages for. In other words, if the gateway is responsible for passing all messages from computers on the subnet with addresses beginning with 172.57, its address must fall in the 172.57.x.x range.

The Whole Setup

A full description of a network components TCP/IP settings are the following 5 settings:

1) IP Address – This is the address of the computer, and must be unique on its subnet.
2) Subnet Mask – Used by the computer to determine if a recipients address is in its own subnet or a different one.
3) Default Gateway – All communication not destined for a computer inside its own subnet is handed off to the gateway for "routing".
4) Primary DNS Server – A way for the computer to take a human readable address like www.microsoft.com and transform it into a number like 207.46.245.230
5) Secondary DNS Server – A backup to the primary DNS server in case it's unreachable.

Not all network components will have or need to have all these fields defined. For example, Cirus Controls spreaders only have an address and a subnet mask defined. It does not need a default gateway because it can only communicate with other machines on its own subnet, and does not need either entry for DNS servers because it cannot take human input to do things like browse the internet or receive mail.

Exceptions

Most computers these days have a setting that “retrieves settings automatically”. This saves the administrator from having to individually set up each computer. It also allows people to just “plug” into a network jack and get a live Internet connection. This works through a protocol called DHCP, or Dynamic Host Control Protocol. Basically, when a computer connects to a physical network, it sends out a broadcast message to any DHCP server listening saying “give me an address please”. If a DHCP server is present on the network, it passes an address, subnet mask, gateway, and DNS servers back to the computer to set up its TCP/IP connection.

Appendix A – Part Number List

WiFi Bridge	DB-04
-Power cable for Bridge	-TS-3001
WiFi Access Point (with cables)	DB-02