CYBERCOMM
BY DC SECURITY PRODUCTS

CyberView™ & CyberStation™

IPTV System Users Manual V3.1

Copyright © 2003 by DC Security Products, Inc. All Rights reserved.

CyberStation™ and ***CyberView***™ are trademarks of DC Security Products, inc.

No part of this product or related documentation may be reproduced in any form without written authorization of DC Security Products, Inc.

This document, ***CyberStation***™ system modules, and ***Cyber View***™ software are subject to change without notice.

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Chapter 1
Overview

This manual provides simple configurations for users, who are unfamiliar with the *CyberStation*™ product family.

An IPTV System consists of:

- *CyberStation*™—The remote controller, located on the customer surveilled premises. *CyberStation's* basic function is to transmit and eventually record video. It is also called **the controller**.
- *CyberView*™—The **video management software suite** for *CyberStation*™. *CyberView*™ displays video from one or more remote controllers. *CyberView*™ also receives and displays the alarms generated. It is also called the **receiver**.

1.1 Terms

In this manual, the terms receiver, video management software, software suite, application or *CyberView*™ are used interchangeably to identify *CyberView*™. The terms, transmitter, remote controller or *CyberStation*™ are used interchangeably to identify *CyberStation*™.

1.2 Chapter description

The chapters are organized as described below.

Chapters 1—4

Chapters 1—4 introduce *CyberStation*™ and provide step-by-step procedures for:

- installing and configuring a *CyberStation*™ to accept connections from *CyberView*™, using Ethernet LAN, DSL and Modem communications.
- installing and configuring *CyberView*™ for a PC to connect to one or more *CyberStations*.
- making connections from *CyberView*™ to *CyberStation(s)* to view real-time video from cameras connected to *CyberStation*™ when both systems are connected to the same Ethernet LAN.
- making connections from *CyberView*™ to *CyberStation*™ to view real-time video from cameras connected to the *CyberStation*™ when both systems are connected by PPP Protocol (modems) over the PSTN network.

Chapter 5

Chapter 5 gives a practical example based on a typical installation.

1.3 Prerequisites

Users familiar with basic ethernet (LAN) and wide area networks (WAN) communication concepts, their terminology, and basic Internet technology, including browsers, will find this manual easier to understand and follow. This manual does not describe the LAN/WAN networking concepts related to *CyberStation*™ operation. Preferably, users should also be familiar with PPP, DSL, and TCP/IP concepts in Microsoft® Windows operating systems.

Users familiar with networks (WAN) communication concepts are invited to thoroughly read this manual for installation, configuration information and procedures of *CyberStation*™.

1.4 Equipment and system requirements

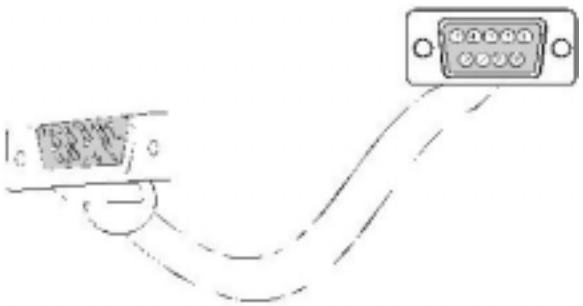
A working IPTV configuration set-up requires the following equipment:

- a *CyberStation*™ remote controller.
- *CyberView*™ software and documentation distribution CD.
- an RS232 connection cable (one DB9 male and one DB9 female connectors in each end).
- a Crossed RJ45 Category 5 Ethernet cable ***or*** an existing Ethernet LAN with at least two RJ45 ports available in an Ethernet Hub or Switch.
- one DSL phone line for high speed communication, and a DSL router/bridge with a multiple port Hub/Switch with at least at least two available RJ45 ports.
- one phone line with dialup communication access for use with the Securcomm *Uniflex DC336B Optional Modem Module* and *CommPort232*. One Telco cable (length as required) and Serial (DB 25 male to DB 25 female) cable.

A working configuration set-up requires these system requirements:

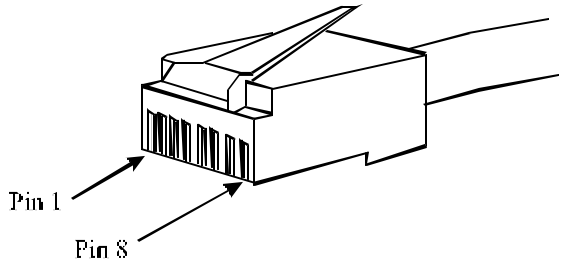
- Pentium II processor with 128 Mb RAM.
- Windows® XP, 95, 98, NT or 2000).
- an Internet browser, such as Netscape Navigator or Microsoft® Explorer.
- a 10 Mbps or 10/100 ethernet interface[1].

[1] Since *CyberStation*™ Ethernet interface is 10Mbps, it should not be connected to “exclusive 100Mbps” LAN devices, because no communications will be possible.



RS232 cable

	DB9 male	–	DB9 female
RXD	2	to	2
TXD	3	to	3
GND	5	to	5



Crossed Ethernet cable

	RJ45 male	–	RJ45 male
TXD	1	to	3
TXD	2	to	6
RXD	3	to	1
RXD	6	to	2

FIGURE 1. CABLES PIN OUT: RS232 AND CROSSES ETHERNET

1.5 Documentation review

Users should read the *CyberStation*™ Reference Manual, available on the enclosed *CyberStation*™ CD, to become familiar with the *CyberStation*™ family of system modules and product features. This documentation is distributed in PDF format. PDF documents can be read using the Adobe Acrobat Reader.

The *CyberStation*™ CD contains the following documentation in English:

- *IPTV*™ *System* User Manual. (*IPTV*™_system_user_manual.pdf, this document).
- *CyberView*™ User Manual. (*CyberView*™_user_manual.pdf).
- *CyberStation*™ Reference Manual. (*CyberStation*™_reference_manual.pdf).

As previously indicated, this manual is intended for initial contact with *CyberStation*™. To fully understand the extensive features and capabilities of the system, and to install and configure *CyberStation*™ for customers with several systems connected corporate networks of any size, it is strongly suggested that the user utilize all the product documentation available on this CD, such as:

- ***CyberView*™ User Manual**. A detailed description of the *CyberView*™ operation.
- ***CyberStation*™ Reference Manual**. An introductory tutorial explaining *CyberStation*™ concepts and its building blocks. It is also a reference manual for configuration and management concepts and commands. The *CyberStation* Reference Manual introduces hardware components, describes cabling, power, other requirements, and other *CyberStation*™ models.

1.6 Document conventions

CyberView™ and *CyberStation*™ documentation uses the following conventions:

Convention	*Description*
`Courier bold`	Keywords and Commands
(Substitute)	Variables that must be replaced by their value. Variables may also be displayed in italics.
< Optional >	Optional arguments or keywords.
{ x | y | z }	One of many options must be selected.
{ x + y + z }	One, more or all options can be selected.
Courier	Text displayed on the display monitor.
`Courier italic`	Examples of information that must be entered.
Listing	*CyberStation*™ configuration listing.
`Button.`	Buttons displayed on screen that can be clicked, using the mouse.
`Field.`	Fields that require the user to enter information into the system.
	Important note.
Type	Key press commands.

Chapter 2
Initial Setup

2.1 Sample configuration

The *CyberStation*™ is shipped from DC Security Products with a default configuration. This default configuration has predefined values, and has no site or user specific values (e.g., dialup phone numbers, IP addresses, alarm conditions, disk recording conditions). Default values are shown on screen if *CyberStation*™configuration is performed using a browser, as described in this manual.

2.1.1 IP addresses and numbers used in the examples

Figure 2 and Figure 3 display the physical connections and the configuration parameter values used as examples.

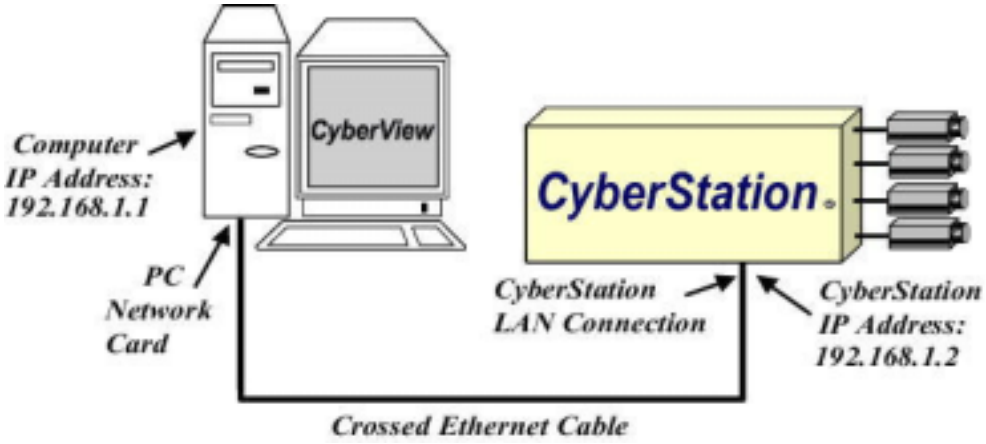


FIGURE 2. IP ADDRESSES EXAMPLE FOR THE LAN CONNECTION

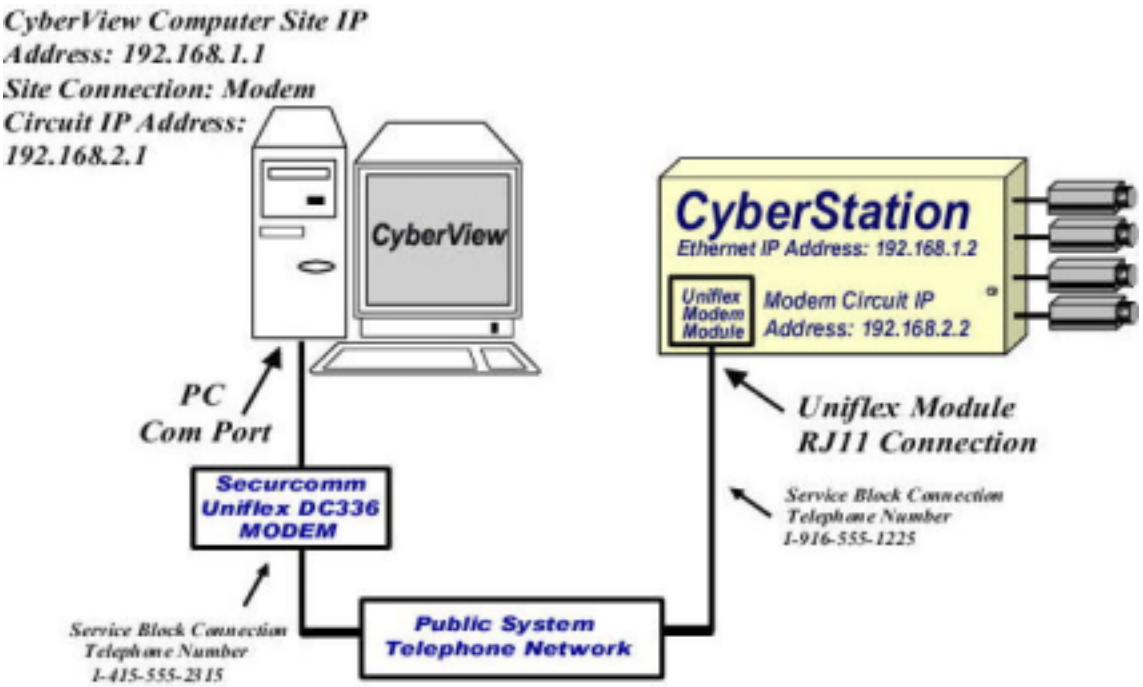


FIGURE 3. IP ADDRESSES EXAMPLE FOR THE MODEM CONNECTION

Figure 2 displays example values (IP addresses) used in this step-by-step procedure for LAN connection configuration. Figure 3 displays example values used in this step-by-step procedure for the MODEM connection.

These IP addresses are Internet private, class C addresses for intranet use, and are not used on the public Internet. For these class C addresses, the network mask is 255.255.255.0.

2.1.2 Username and passwords

When delivered from DC Security Products, *CyberStation*™ system software has a default username and password. Users are encouraged to change those values when the *CyberStation*™ system starts working in a customer site.

Default values are:

- Username: **`hello`**
- Password: **`world`**

`hello/world` has administrator privileges.

As an added security measure, *CyberStation™ IPTV CFGMain* program will delete this account as soon as a new username/password is created and entered in the Remote Controller. *CyberView™,* the Video Management Software suite, will **not** delete this account because it is managed in a safe and autonymous environment.

The procedures described in this chapter assume the use of the default settings.

2.2 Getting Started…..First-time *CyberStation™* IP address configuration programming

To provide an IP address to the *CyberStation™* for first-time use proceed with the following steps:

1. Connect a PC to the *CyberStation™* console port (serial-0), as shown Figure 4 (see Figure 1 for cable pin out details).

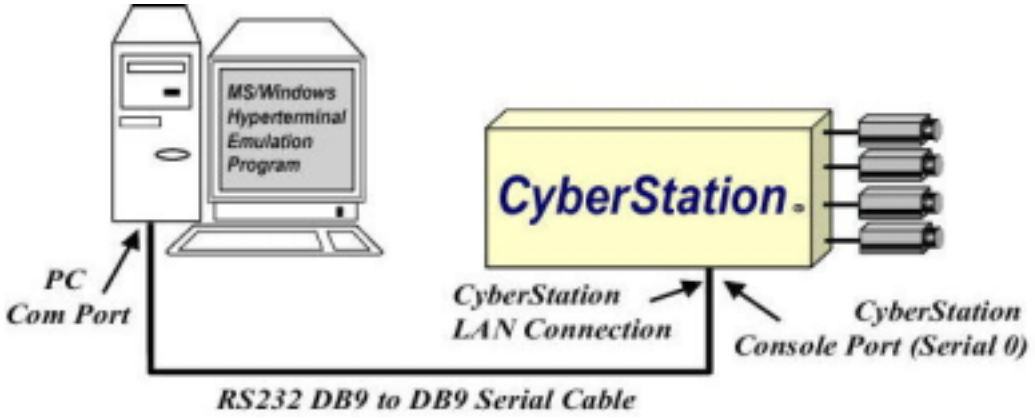


FIGURE 4. PROVIDING AN IP ADDRESS TO *CYBERSTATION™*

2. Set HyperTerminal parameters, as shown in Table 1: HyperTerminal Parameters.

Table 1: HyperTerminal Parameters

Speed	9.600 bits/s
Parity	None
Data	8 bits
Stop	1 bit
Flow control	None

3. Once the connection is complete, enter the following commands

```
Username: hello                    Username: hello

Password: *****                    Password: world

User and password ok.              User has logged in
Connected
```

4. Press **↵Enter**.

FIGURE 5: LOGGING INTO THE CYBERSTATION USING HYPERMINAL

5. At the `sys>` prompt, type "***cfg run"*** followed by the IP address and the subnet mask command. This action sets up the IP address and the mask in the default file setting.

sys> **cfg run** 192.168.1.2 255.255.255.0 — *Set up Ethernet IP address and the submask*

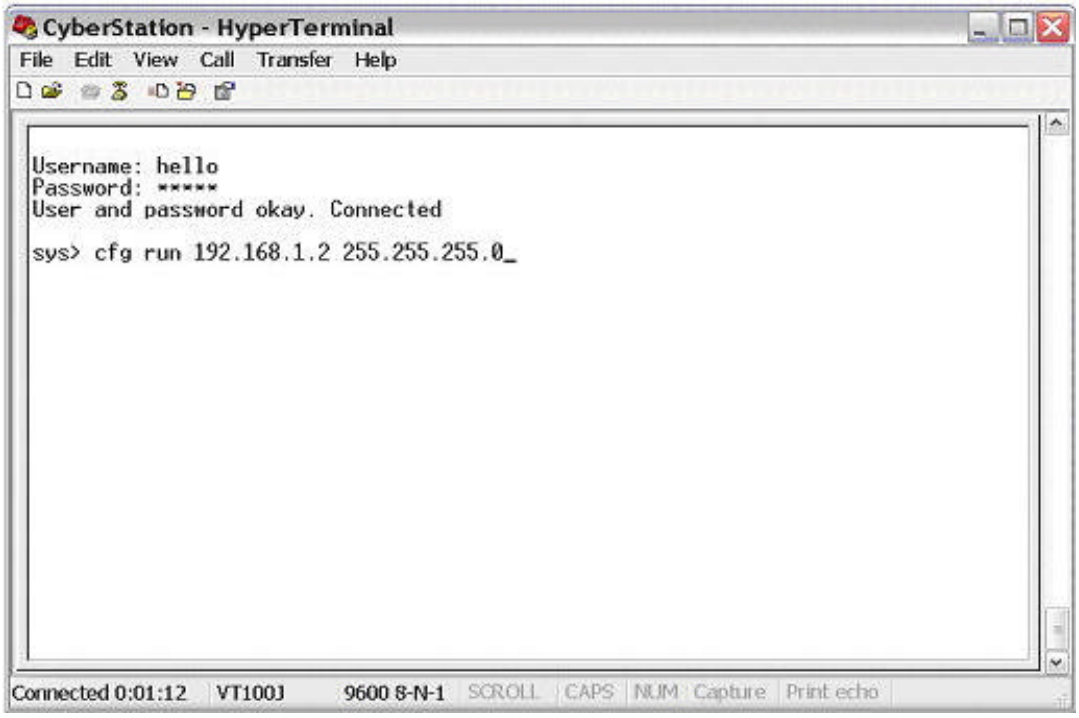


FIGURE 6: ENTERING IP ADDRESS INTO HYPERTERMINAL PROMPT

If the network mask value is not entered, the *CyberStation*'s network mask default value is 255.255.255.0, corresponding to a class C network. For this example the IP address is 192.168.1.2, and the default mask is entered for clarity below.

6. Once the "cfg run <IP Address> & <Subnet Mask>" command is typed and displayed on the screen, press the ↵Enter key to execute the command.

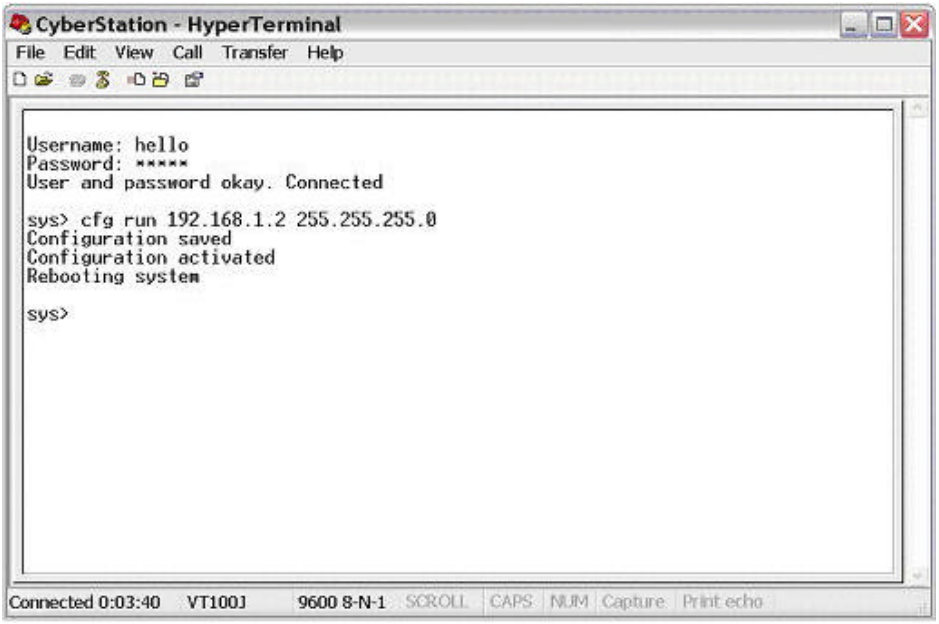


FIGURE 7: HYPERTERMINAL COMMAND SCREEN DISPLAY AFTER DATA ENTRY

When executed, the command the screen displays:

- `Configuration saved`—save changes in the 'default' configuration file
- `Configuration activated`—activates the "default" configuration file
- `Rebooting system`—restarts the *CyberStation*™ Controller to allow the new configuration changes take effect

Once *CyberStation*™ reboots, it is now ethernet accessible, with the proper IP address, until another configuration is entered or the IP address changed.

If a *CyberStation*™ IP address must be changed again, the user can perform the previous procedure, or do the following:

1. Connect to *CyberStation*™ using an internet web browser and accessing the main configuration menu as explained in Section 2.4 Configuring *CyberStation*™ using web-based main configuration menu.
2. Add the new IP address.
3. Exit the web-based main configuration menu.
4. Connect again using the web-based main configuration menu.
5. Delete the old IP address and save the modified configuration.

2.3 Setting the IP address of the PC

While using the appropriate Windows® configuration facilities, set the PC's LAN interface to the value 192.168.1.1. Set network mask to 255.255.255.0. Remember, these values are only for this example, a LAN with two network devices—the PC and the *CyberStation*™. If the PC has more communication interfaces (other LAN devices, Network cards, etc.) connected to the IP network, it may require further configuration changes. If the PC is connected to an existing LAN, refer to the instructions provided in Section *3.1* Connecting the *CyberStation*™ to an existing LAN.

2.4 Configuring *CyberStation*™ using web-based main configuration menu

After setting an IP address to the ethernet interface, *CyberStation*™ can be more easily accessed by the LAN. Both the PC and the *CyberStation*™ should be placed on the same LAN. The connection diagram should resemble one of the diagrams depicted in Figure 8.

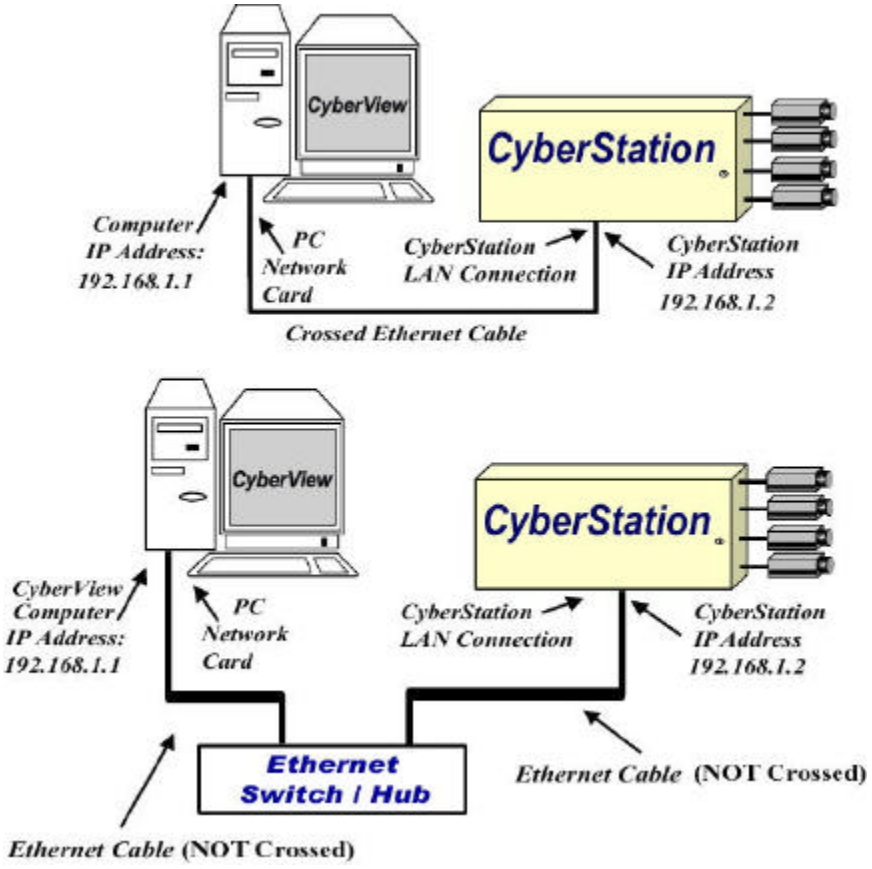


FIGURE 8. CONNECTING THE *CYBERSTATION*™ TO THE LAN

Now the user can access the *CyberStation*™ using an Internet web browser, and configure it with the help of the embedded web-based *CFGMain* configuration utility (or main configuration menu) accessable in *CyberStation*™.

The address entered in the URL field should follow this format:

`http:// <CyberStation-IP-address>/config.html.`

For this example, type this address in the URL field:
`http://192.168.1.2/config.html.` The *CyberStation*™ login dialog box appears.

Follow these steps to continue configuring the *CyberStation*™, using the web-based main configuation utility:

1. Type *`hello`* in the **`User Name`** field and *`world`* in the **`Password`** field. The Main Configuration Menu screen appears.

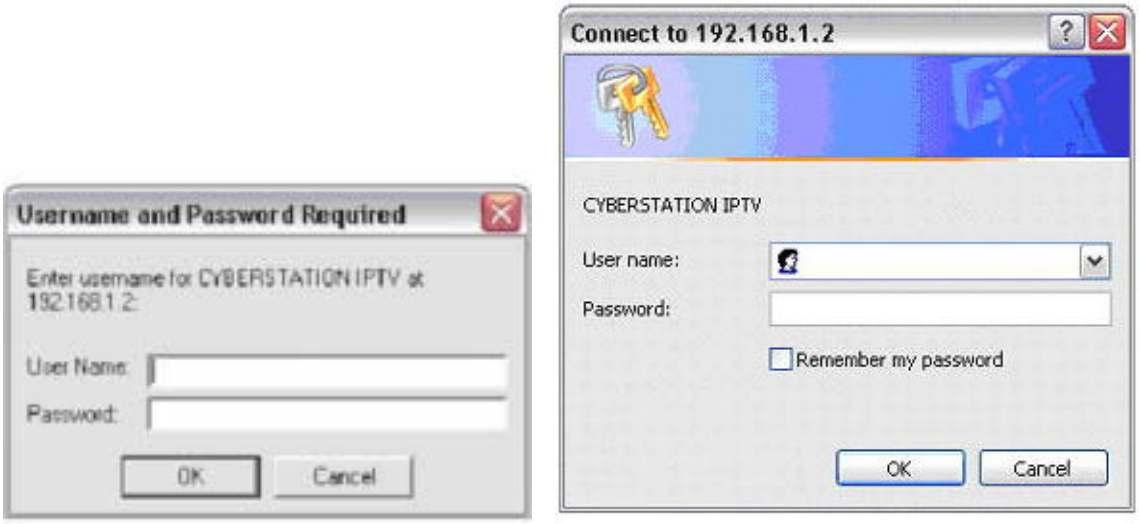


FIGURE 9. REQUIRED PASSWORD TEXT BOXES FOR ACCESS TO THE SETUP MENU IN THE *CYBERSTATION*™ USING NETSCAPE (LEFT) OR INTERNET EXPLORER (RIGHT) BROWERS

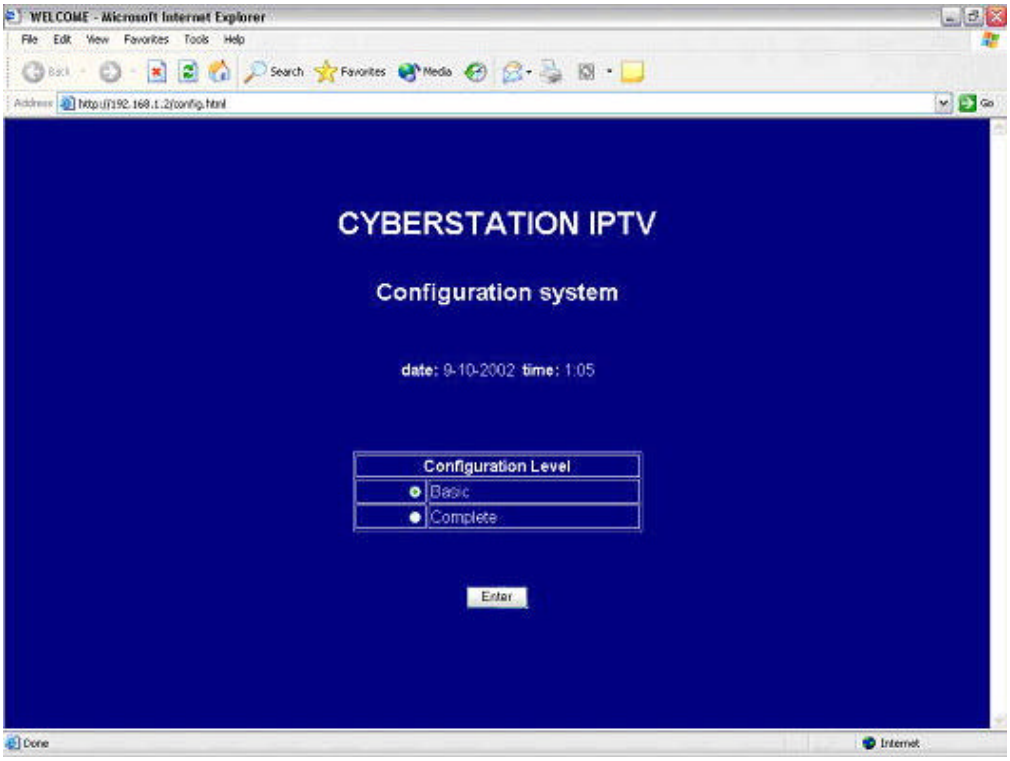


FIGURE 10. MAIN CONFIGURATION SCREEN

2. Select one of two configuration levels, using the radio buttons:

   - **Basic**—allows basic *CyberStation*™ configuration parameters. This option is advisable when either the equipment has a simple configuration, or the user is unfamiliar with the controller's configuration.

   - **Complete**—allows configuration of all *CyberStation*™ parameters. The user can make more complex configurations. Basic parameters appear in white text. Parameters that do not appear when using the basic configuration level appear in yellow text.

3. Click **Enter**. The Main page appears, which contains different system configuration contexts and their descriptions.

The user can now configure any parameter of every context, such as the MODEM context that was utilized when the Modem circuit was defined, as described later in this document.

The Context Selection Main Page is displayed with the various contexts of the system configuration with their descriptions. When viewed in Netscape Navigator or Internet Explorer, the Context Selection Main Page contains the same Context information, but the browsers display contain minor layout differences, as shown in Figure 11.

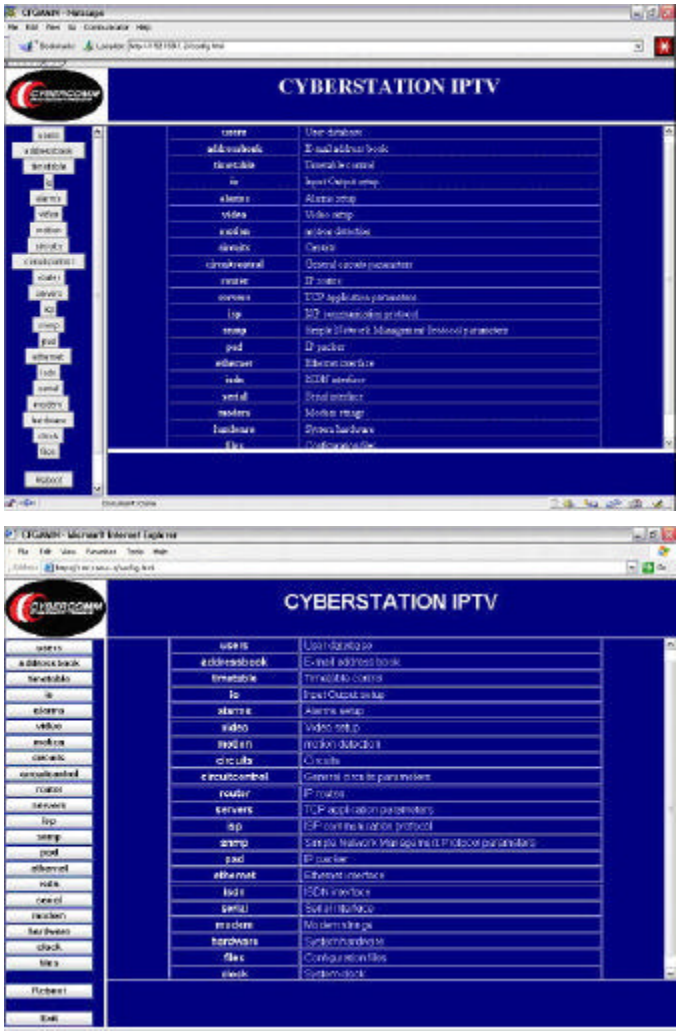


FIGURE 11. CONFIGURATION CONTEXT SCREENS IN NETSCAPE AND INTERNET EXPLORER

2.5 Files context

The files sub-context allows the user to save configurations. This section explains the *CyberStation*™ configuration files.

The *CyberStation*™ can store up to 16 configurations in flash memory. Users can view stored configurations by logging onto the web configuration utility and clicking **`Files`**. As

shown in Figure 12, the form displays existing file names and available options associated with those files. Clicking the radio button to the right of the filename row selects the file.

FIGURE 12. FILE CONFIGURATION SCREEN

Once a file is selected, users have the following options:

- `Delete` deletes the selected file.
- `Show` displays the selected file configuration.
- `Activate` sets an active flag to the selected file. Only one file can be active at any time. The file name is displayed in bold. *CyberStation*™ uses the active file when rebooted. If there is no active file, *CyberStation*™ uses the default configuration file. **If there is no configuration saved with the name "Default", the Remote Controller will startup as it was delivered from the factory**.
- `Save` saves the running configuration to flash memory. The running configuration is loaded when the *CyberStation*™ is first started, including all changes made from the main configuration menu utility. If a name is typed in the `Save as` field and `Save` is clicked, the running configuration and the changes are stored and have the newly assigned name.

- `Main` returns to the main menu.

2.6 The flash memory in the *CyberStation™*

The user has access to the flash memory program files and the hard disk video files using FTP connections to the *CyberStation*™ system. The flash memory folders contain the system software (main-program), configurations (config-files), web pages, javascripts and applets (web-pages), and debugging trace logs (log-files), also available using FTP.

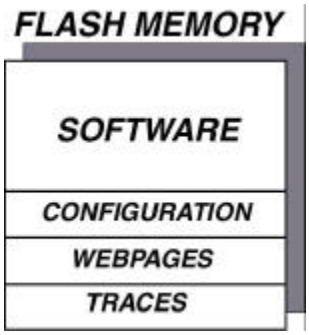


FIGURE 13. FLASH MEMORY LAYOUT

Users can save the *CyberStation*™ configuration to a PC file and restore it in the future if the *CyberStation*™ board must be replaced for any reason. Saving a configuration is perfomed using an FTP application to copy the configuration from the folder config-files in the flash folder of the *CyberStation*™. The FTP application displayed in Figure 14 is SmartFTP, and is currently freeware.

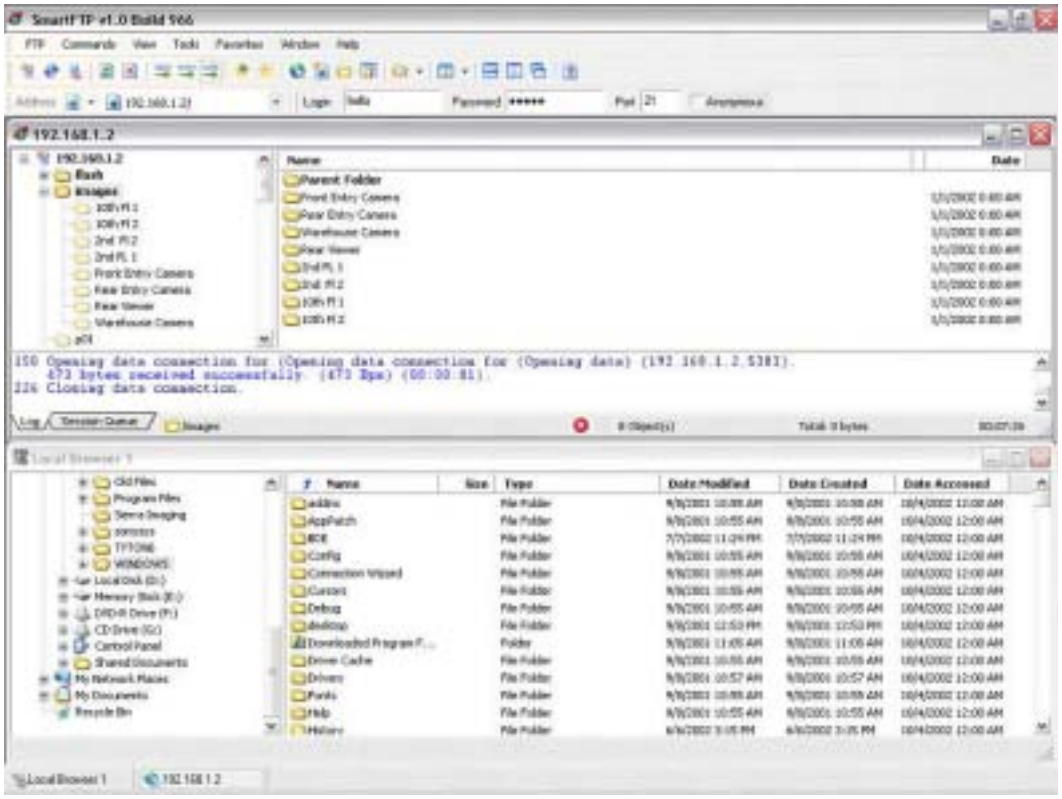


FIGURE 14. ACCESSING THE FLASH MEMORY USING SMARTFTP (A SAMPLE FTP PROGRAM)

CyberStation™ core software updates are performed by transferring the new system software file to the main-program file with FTP. When new software or software updates become available, visit our web site at http://www.dcsecurityproducts.com/ to aquire any future updates. When the new software update transfer is completed, the system automatically reboots. Do **not** power down during this operation, otherwise the *CyberStation*™ becomes unusable and must be returned to the factory to be reloaded for an additional charge. The ServerBus/Input8 (IOP) module system software is contained within the hitachi-program folder and is updated using the same procedure. Web pages are loaded in the same manner.

2.7 Installing *CyberView*™ in the PC

To install *CyberView*™, locate the Add/Remove Software Icon in the Control Panel of your Windows® operating system, and follow the instructions below.

2.7.1 *CyberView*™ installation on Windows® 95 / 98

1. If applicable, uninstall the previous version of *CyberView*™. If using a LAN connection, install an ethernet card and configure the TCP/IP protocol. If using a WAN connection, install a Modem Card or a compatible Exterior Modem and the Dial-up Networking.

2. Execute **`setup.exe`** and follow the instructions.

3. When the installation is complete, click the *CyberView*™ icon to launch the application. The icon is located on the desktop. A dialog box appears with a message to reboot the PC.After rebooting the PC, click the *CyberView*™ icon to launch the application. The login dialog box appears. Enter the default username and password in the fields:

   - **`hello`** : ***USERNAME***
   - **`world`** : ***PASSWORD***

2.7.2 *CyberView*™ installation on Windows® NT4.0 / 2000 /XP

1. If applicable, unistall the previous version of *CyberView*™.If using a LAN connection, install an ethernet card and configured the TCP/IP protocol. If using a WAN connection, install a Modem Card or Exterior Modem and the Remote Access Server.

2. Execute **`setup.exe`** and follow the instructions.

3. After rebooting the PC (if required), click on the *CyberView*™ icon to launch the software application. The login dialog box appears. Enter the default username and password in the fields:

   - **`hello`** : ***USERNAME***
   - **`world`** : ***PASSWORD***

2.7.3 *CyberView*™ installation on Windows® Me

1. If applicable, unistall the previous version of *CyberView*™. If using a LAN connection, install an Ethernet card and configure the TCP/IP protocol. If using a WAN connection, install a Modem Card or Exterior Modem and the Remote Access Server. When the installation is complete, right-click the *CyberView*™ icon located on the desktop and click `Properties.`

FIGURE 15. *CYBERVIEW*™ ICON WINDOW

2. Click the `Memory` tab as displayed in Figure 16.

3. Click the `Initial Environment` drop-down menu, and set the initial environment size to `512`.

FIGURE 16. MEMORY SCREEN

4. Click “Apply”, then “OK” to accept the changes. Click the *CyberView*™ icon. A dialog box appears with a message to reboot the PC, if required. After rebooting the PC, click the *CyberView*™ icon to launch the application. The login dialog box appears.

5. Enter the default username and password in the fields:

   - `hello` : ***USERNAME***
   - `world` : ***PASSWORD***

Because *CyberView*™ was originally developed as a bilingual application (Spanish/English), it automatically detects the language configured on the PC. Although the English version is the executed language configured on the PC, some DOS data remains in Spanish and occasionally appears. Currently, there is no remedy for these occurances.

2.8 Utility software

These freeware and shareware tools and applications are helpful when using *CyberView*™.

- The FTP Client Protocol is used to make software updates, and these updates are available at http://www.dcsecurityproducts.com in the *CyberStation*™ ™ Updates section. Some available fee-based, freeware, and shareware tools and applications
  - WS_FTP LE: http://www.ipswitch.com.
  - SmartFTP: http://www.smartftp.com.
  - CuteFTP: http://www.cuteftp.com
  - Microsoft’s own FTP client software http://www.microsoft.com.
  - TeraTerm: http://ftp.riken.go.jp.
  - QVT/Term: http://www.qpc.com.

Internet Browsers with applets to access *CyberStation*™:

- Netscape Communicator: http://www.netscape.com.
- Microsoft® Internet Explorer: http://www.microsoft.com.

Chapter 3
CyberStation™ and CyberView™ in LAN

This chapter describes connecting *CyberStation*™ and *CyberView*™ over a LAN. For a simple and basic system, we recommend using a single crossed ethernet cable. The resulting basic ethernet LAN has two devices. This ensures that no conflicts related to TCP/IP addressing arise. We also recommend that users unfamiliar with TCP/IP technology begin with this "two devices" LAN configuration to configure the remote controller.

3.1 Connecting the *CyberStation™* to an existing LAN

When the *CyberStation*™ and/or the PC with *CyberView*™ connects to an existing LAN, the user must first request the IP address and Network Masks from the person responsible for assigning IP addresses. This person is usually the communication or IT manager.

Users should be aware that with some LANs, the servers act as DHCP servers (or equivalent), and automatically assigns IP addresses. In this case, it is even more important to ask the communication manager's involvement in the IP address assignment for *CyberStation*™ and the PC host of *CyberView*™. *The CyberStation*™ IP address cannot be assigned dynamically by the DHCP server. It must have a **fixed** IP address set up during the configuration process. The PC's LAN card IP address must also be **fixed** if the PC is to receive alarms.

If routers are installed in the LAN, it may be necessary to configure the `Router` context in the *CyberStation's*™ CFGMain. The same type of router configuring may be necessary for the PC with *CyberView*™. If required, this operation should be performed by qualified network personnel and is outside the scope of this manual.

3.2 Configuring a LAN site in *CyberView™*

After configuring the *CyberView*™ to an existing LAN, the user is ready to configure *CyberView*™ to access the *CyberStation*™ using the LAN connection. The *CyberStation*™ must be identified by a name. In this example, it is ***Dallas Branch***, as shown in Figure 17.

To give the *CyberStation*™ a name:

1. Log onto the application with the default username and password (**`hello/world`**). The *CyberStation*™ main screen appears. This default account has full privileges. We strongly recommend that users create a new account with full privileges and delete the default.

Login and password must correspond to a valid *CyberStation*™ username and password. For now, our example uses **`hello/world`**. In the sample configuration in Chapter 6, login/password is **`dallas/12345.`**

2. Click the **`Sites`** tab. A screen similar to Figure 18 appears.

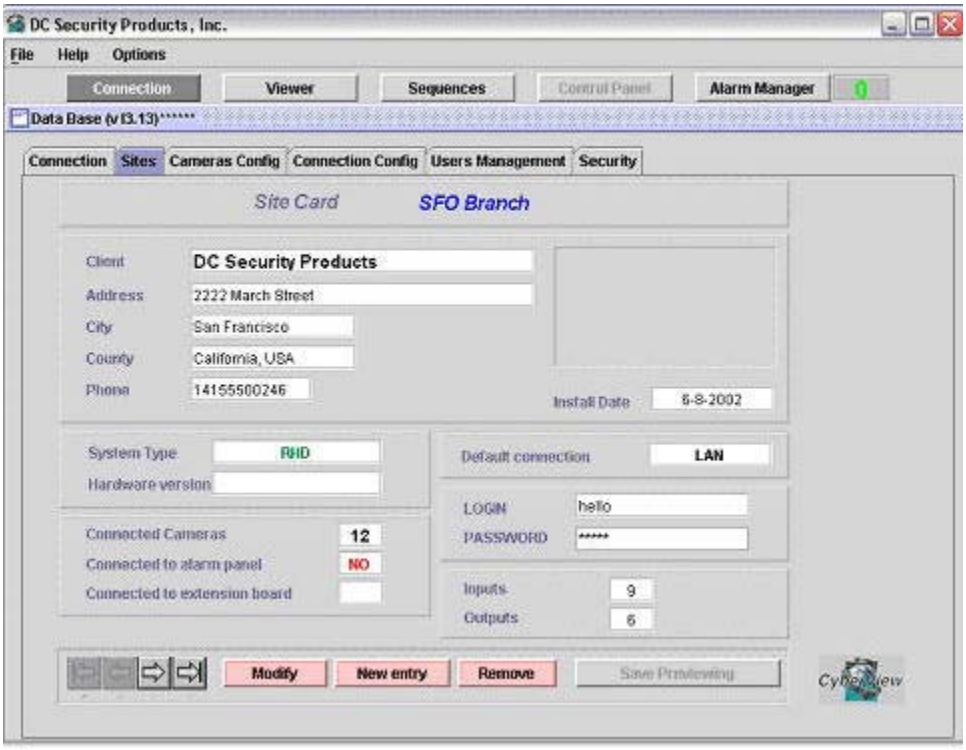


FIGURE 18. SITES SCREEN

3. Click `New entry` to create an account for the new *CyberStation*™. The `Site Configuration` window appears, as shown in Figure 19, allowing users to enter site information.

4. Enter the specific site information into the fields:

   - `Site name`
   - `Connection to site login`
   - `Connection password`
   - `Connected cameras`

In the site information section, it is recommended that the State and Country be located in the same text box (ie Utah, USA or California, USA etc). This will insure less confusion when reviewing site information.

5. Click `Add` to create the new account. The application adds the new site and automatically opens the connection window to define a communication setting(s) to the new site, as shown in Figure 20.

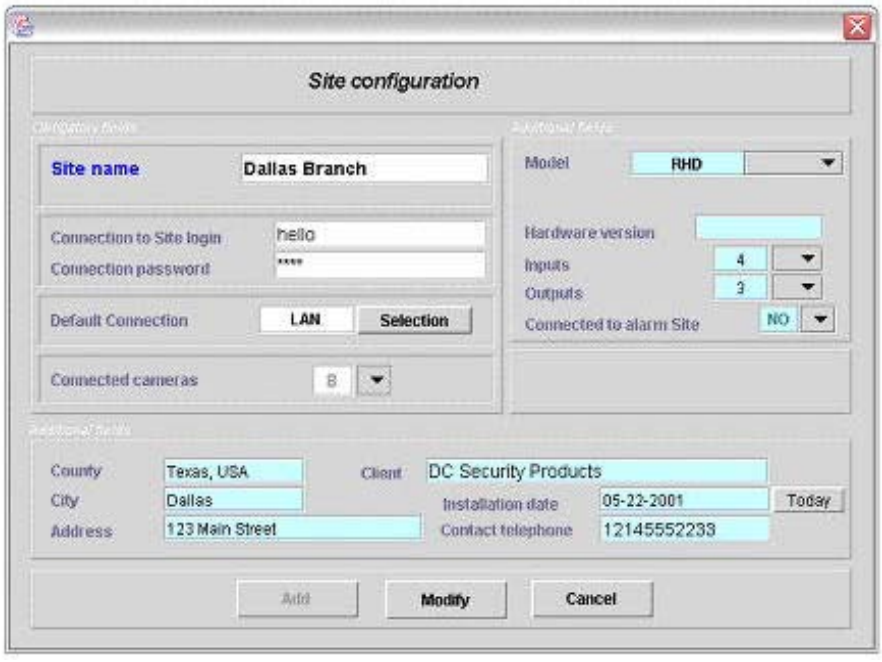


FIGURE 19. CONFIGURING A NEW SITE

6. Enter the required information in the `Connection type` and `IP Address` data fields.

7. Click **Accept** to create the connection.

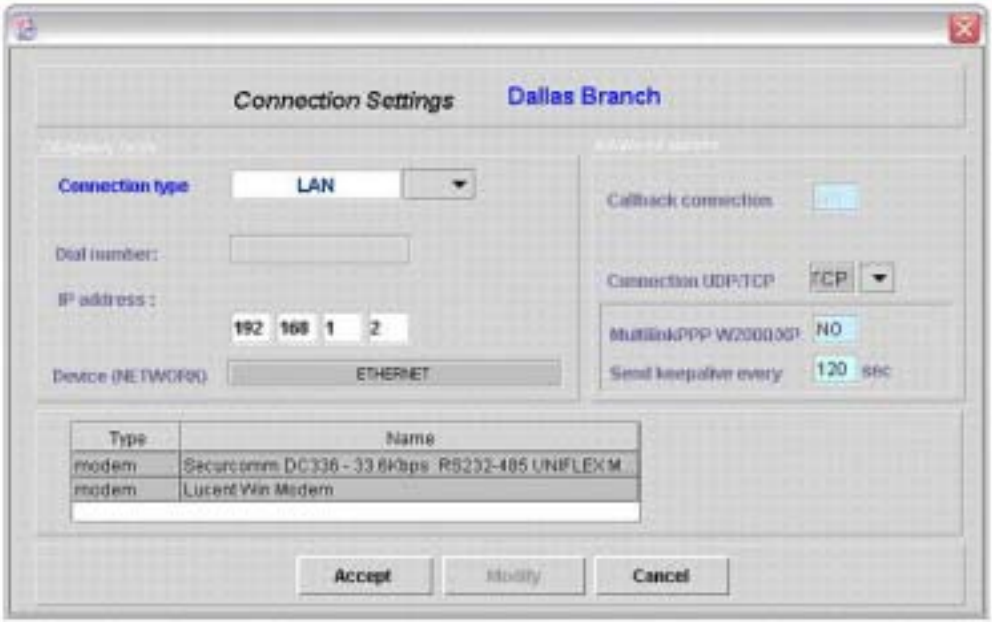


FIGURE 20. CONFIGURING THE NEW CONNECTION

The main menu now has a new entry with a site named `Dallas Branch` as shown in Figure 20.

By selecting the **Dallas Branch** site and clicking **Connect/Disconnect**, *CyberView*™ enables the connection. Users can now see video (clicking **Viewer**) from any connected (and properly configured) cameras.

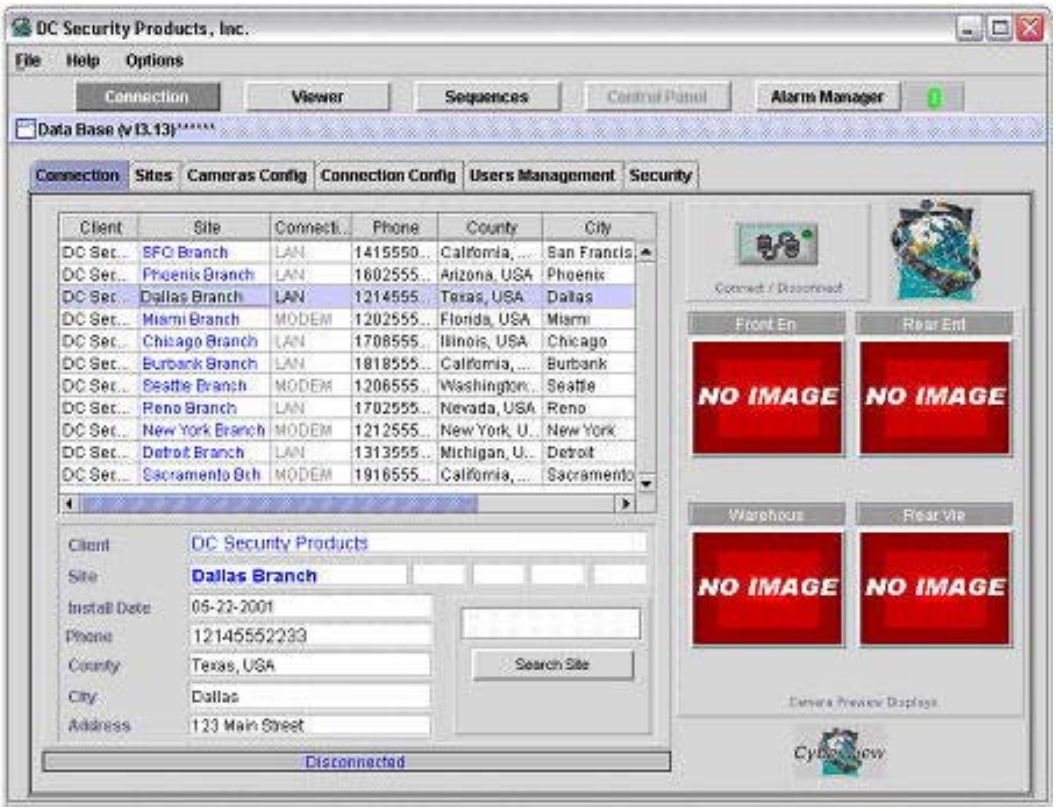


FIGURE 21. CONNECTION SCREEN

Chapter 4
CyberStation™ and CyberView™ in Dialup

4.1 Configuring the Modem circuit in *CyberStation™*

In *CyberStation*™ terminology, WAN connections are configured as Circuits. To configure the simplest MODEM circuit the user should proceed as described below, using the web-based main configuration menu utility. To access the web-based main configuration menu utility, the user should review information contained in Section 2.4 Configuring *CyberStation*™ using web-based main configuration menu, which is elaborated here.

To access *CyberStation*™*'s* Main Configuration Menu, the user must enter the URL in this format in the browser's URL field:

http:// <CyberStation-IP-address>/config.htm

In this example the address is `http://192.168.1.2/config.html`. Enter "*hello*" in the **Username** field and "*world*" in the **Password** field.

The *CFGMain* Configuration Menu contains various Configuration Contexts identified and access with buttons. After clicking on **Circuits** (the Circuits Context), a request to enter a new circuit, to be identified by a name is shown. Once a name is entered (our example is **MODEM**), a table appears, allowing users to set all necessary configuration parameters, while showing their default values. The user must set the required values, as indicated in Figure 22.

It is important to emphasize that each communication circuit created (ISDN, MODEM, or LAN) will require their own Subnetted IP Address or what we call an IP Circuit Tunnel. This tunnel will need an address not shared with other paths (for example, 192.168.**1**.2 [LAN] or 192.168.**2**.2 [MODEM] or 192.168.**3**.2 [ISDN] in each each example, the IP Address displays an underlined different third octet highlighting the unique subnetted family of IP addresses necessary for proper TCP/IP network communication). Users are also required to configure the proper *CyberStation*™ hardware modules used by the circuit. Each IP Circuit Tunnel is there to provide a data path over which IP packets of information can travel to the approved user requesting the information. Although the core IP Address of the *CyberStation*™ is configured in the **Lan** Context, each additional IP Circuit Tunnel is created in the **Circuits** context for flawless operation. In our example, you will need to configure the **Circuits**, **Serial**, **Modem**, and **Hardware** contexts sub-menus which are contained in the CFGMain Configuration Program. Additional information on these and the other configuration contexts is available in the *CyberStation*™ Reference Manual included on our Introduction CD.

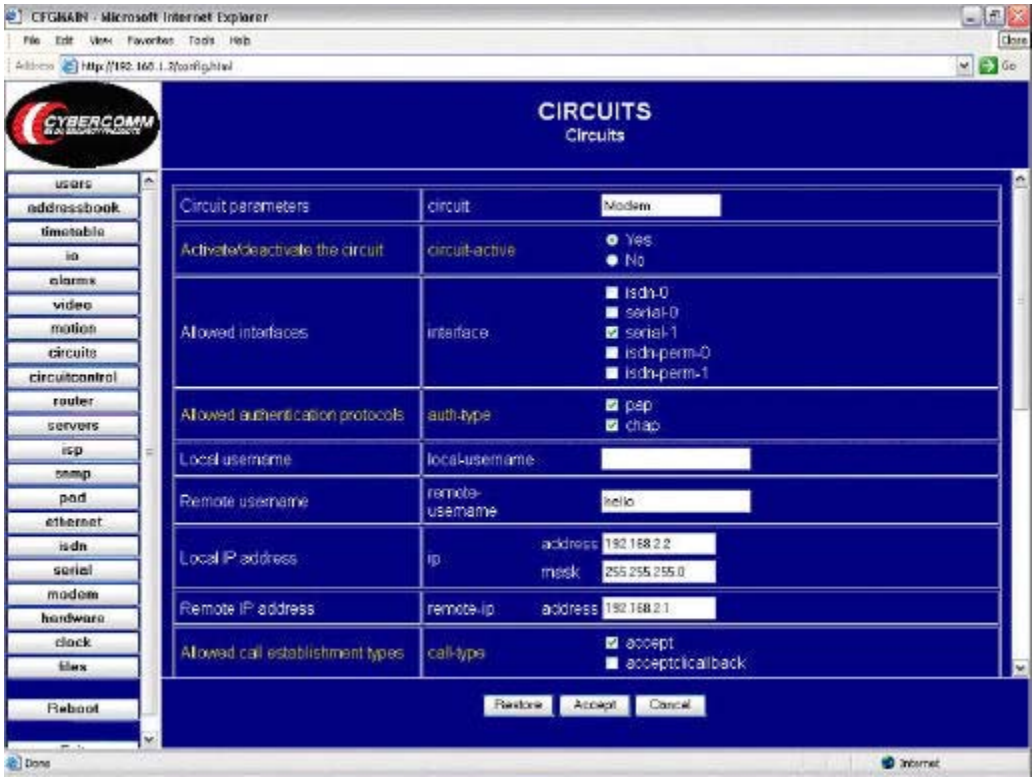


FIGURE 22. CONFIGURING THE MODEM CIRCUIT

The remaining parameters can be left with their default values.

With this circuit set, when properly plugged to the PSTN network, the *CyberStation*™ will:

- answer any Modem data call received (e.g., a connection originated in a properly configured *CyberView*™).
- negotiate a ppp, pap, or chap authentication procedure. If username and password are correct (**`hello/world`**), a TCP/IP-PPP connection is set up.
- sustain a TCP/IP connection with the Modem device attached to the *CyberView*™ with a unique subnet between the two devices.

If no IP packets are sent or received for longer than 180 seconds, the remote controller clears the initiated call.

4.2 Saving the new configuration

The modified configuration, including the new MODEM circuit, is the currently running configuration. Before the new configuration can be used, it must be saved to flash memory and activated to load when the system restarts.

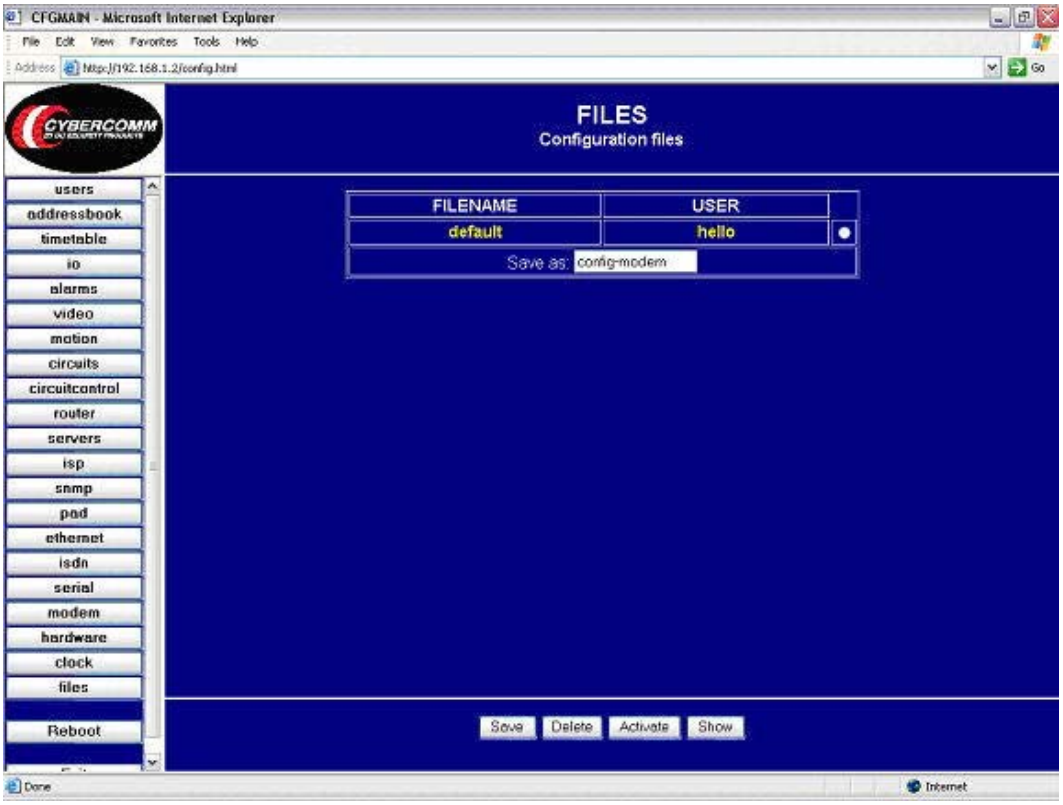


FIGURE 23. SAVING A NEW CONFIGURATION

To save the new configuration to flash memory:

1. Click on the `files` (Files) context.
2. Type a name for the new configuration (our example is *config-Modem*) in the `Save as` field.
3. Click `Save` to store it.

Once this action is complete, the new configuration (*config-Modem*) is saved to flash memory.

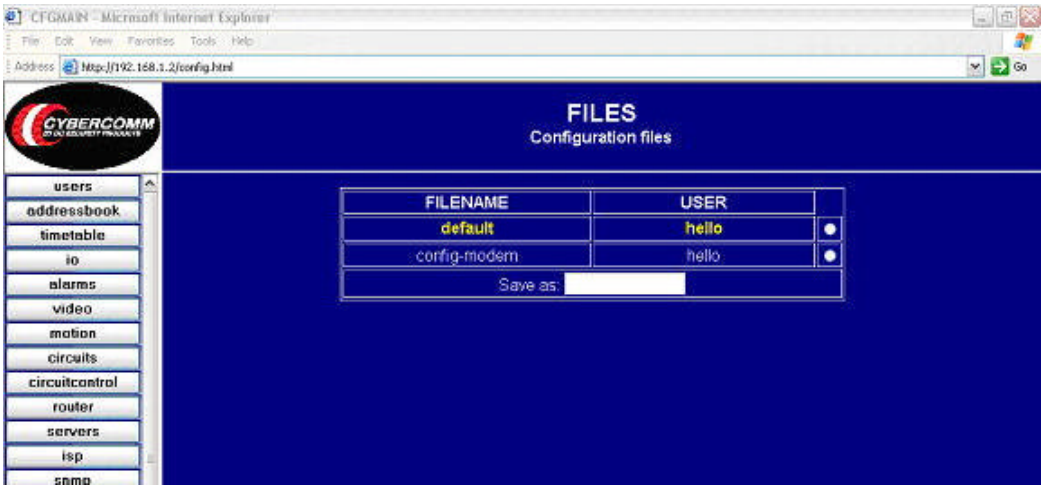


FIGURE 24. CONFIG-MODEM CONFIGURATION SAVED

There are now two configuration files (*default and config-modem*) stored in flash memory. To activate the *config-modem* configuration:

1. Click the radio button to the right of *config-modem* to select it.

2. Click **Activate** .The file *config-modem,* is flagged as active. Its filename and user is highlighted in gold lettering.

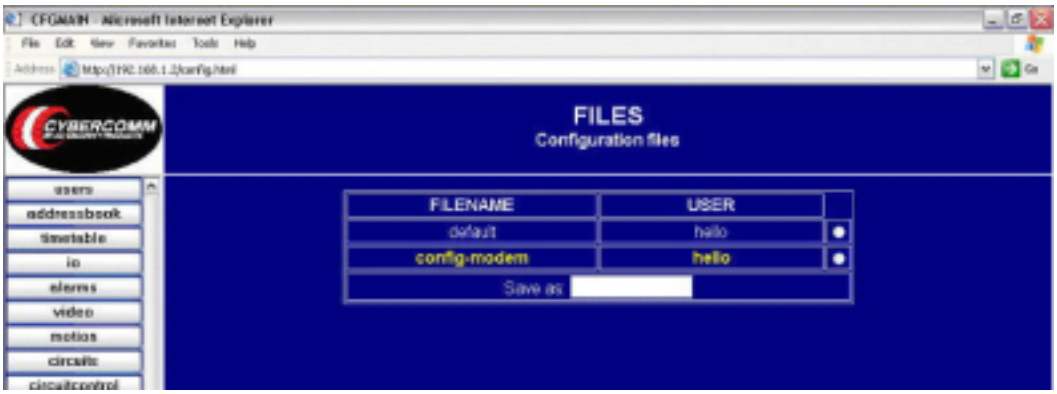


FIGURE 25. CONFIG-MODEM CONFIGURATION ACTIVATED

3. Click **Reboot** to restart *CyberStation*™ using the configuration file selected as **active** (*config-modem* highlighted in gold).

Once the reboot sequence is completed, the Main page returns. A new dialup analog circuit named ***modem*** is now added to our existing *CyberStation*™ configuration, and renamed as a new additional file.

4.3 Viewing the new configuration

Users can dispay any configuration shown in the files context for review. To list the desired configuration, select the radio button to its right, and then click **Show** . If the user selects the configuration *config-modem*, the web configuration utility displays:

```
circuits
        circuit modem
                interface serial-0
                auth-type pap+chap
                remote-username hello
                ip address 192.168.2.2 mask 255.255.255.0
                remote-ip address 192.168.2.1
                call-type accept

circuitcontrol
                multilink active yes

ethernet
        !mac address 00D00A:000024
        ip address 192.168.1.2 mask 255.255.255.0
```

4.4 PC MODEM adapter installation and configuration

To properly access the *CyberStation™'s* optional *Securcomm Uniflex DC336B* using a modem connection from the PC containing *CyberView™,* that PC must have a properly installed, configured and compatible modem adapter. The adapter must be compatible with Windows® Dial-Up Networking from Microsoft®. Please refer to the modem device's installation manual. For optimum performance, DC Security Products recommends the *Securcomm Uniflex DC336* Desktop Modems.

It is important to remember that video transmission of images using dialup modems are at speeds of 1 to 2 images per second, which to some may be slow. We recommend that users investigate faster forms of WAN transmission (DSL, ISDN or Cable) where possible. Using faster technologies requires the use of a Static IP that supports Network Address Translation (NAT), provided by your Internet Service Provider. You will also require a DSL Router/Bridge or ISDN Router/Bridge for high speed WAN communication depending on choice. For dynamic IP use, please contact your *CyberStation™* Distributor or DC Security Products for further information.

4.5 Configuring a remote site modem connection in *CyberView™*

Having followed all previous steps, the user is now ready to configure *CyberView*™ to access the *CyberStation*™ using the modem connection. To do so, a new connection must be defined in the database. Since Dallas Branch has a LAN entry in the database only the new modem connection must be defined.

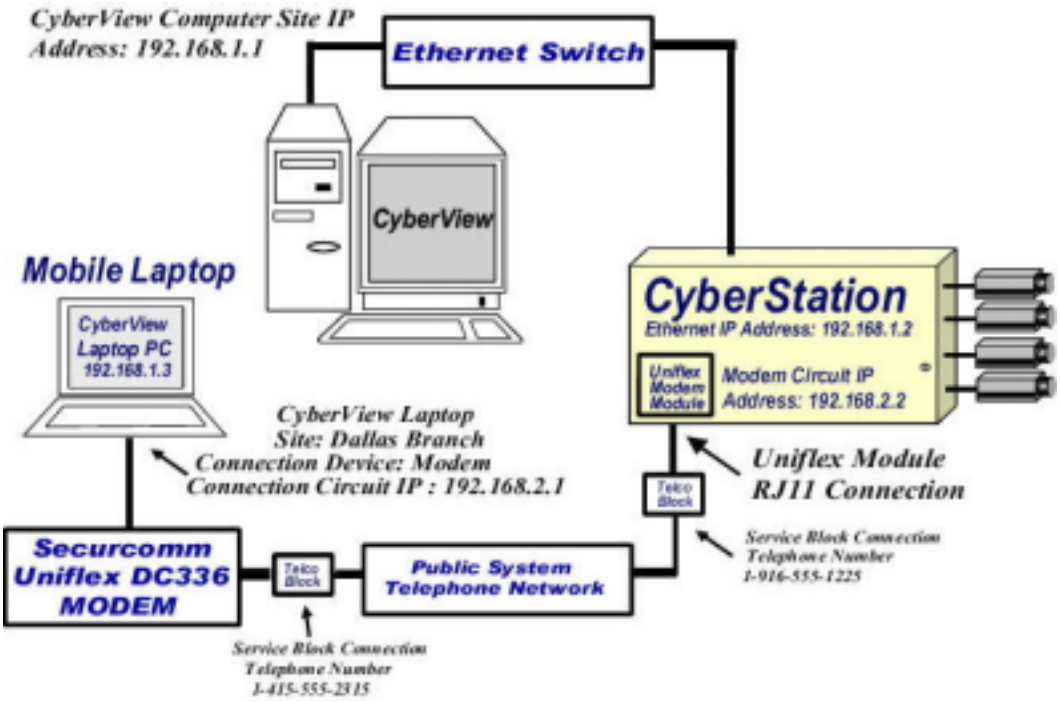


FIGURE 26. CONNECTING TO A REMOTE SITE THROUGH MODEMS WITH *CYBERVIEW*™

To configure the new connection in Dallas Branch, enter the indicated values:

1. Locate the **Connection Config** tab of Dallas Branch, The ethernet-LAN connection form configured in Chapter 3 is displayed. (see Figure 27).

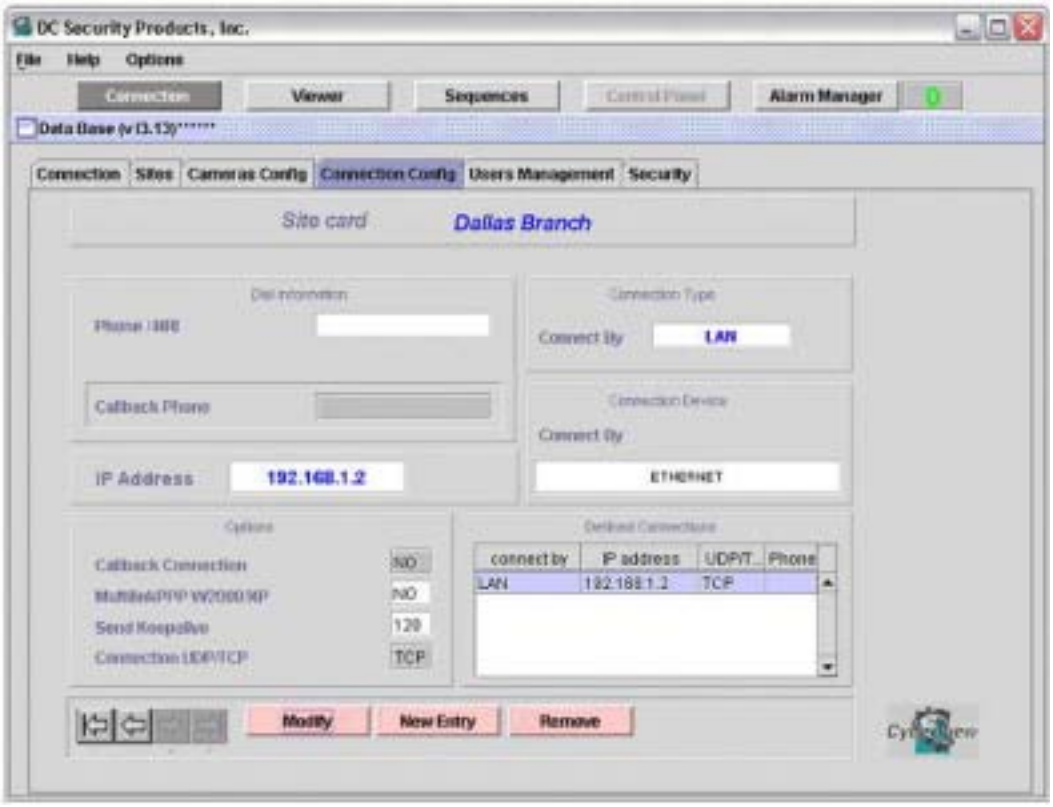


FIGURE 27. DALLAS BRANCH LAN CONNECTION

2. Click New Entry and configure a new modem connection, as shown in Figure 28. Proceed as shown in Figure 28:

3. In **Connection type**, select **MODEM**

4. **Dial number** is set to `12145552333`. This is the phone number of the telco block where the *CyberStation*™ Modem module is plugged.

5. The **IP address** entered is the IP address of the *CyberStation*™ Modem port.

6. The `Device (Modem)` is the name Windows® assigns to the Modem unit. *CyberView*™ reads this information from the Windows® registry. The user has to select the name of the Modem device.

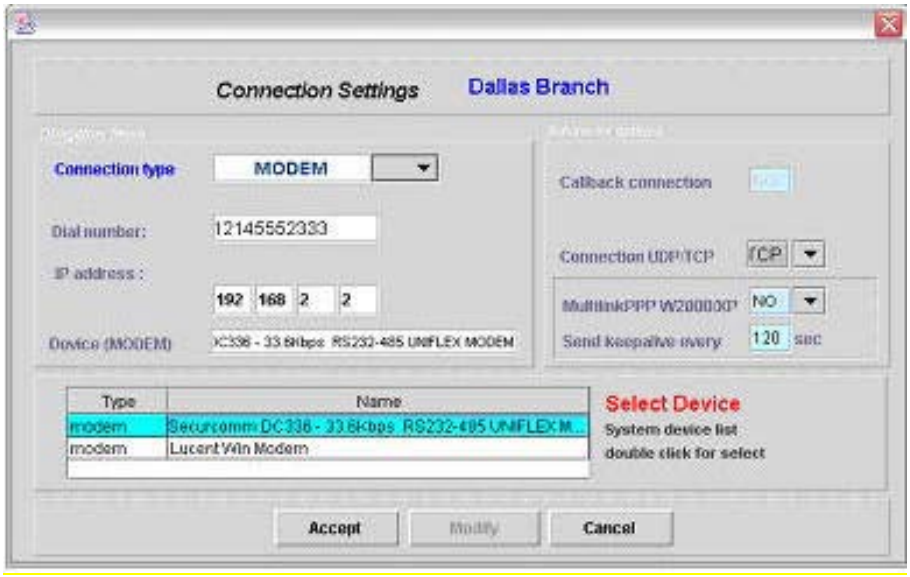


FIGURE 28. CONFIGURATION OF MODEM CONNECTION

7. Define the Dallas Branch modem connection as default. To do it, locate the `Sites` tab, and click `Modify`:

8. In the `Default Connection` dialog box, click the `Selection` button. The Treatment window appears, providing the available communication choices programmed for this site. Select MODEM.

FIGURE 29. CONFIGURING THE MODEM CONNECTION AS DEFAULT

If properly configured, Dallas Branch will be displayed in the `Connection` tab and the user can make MODEM and LAN calls to the *CyberStation*™ from *CyberView*™, changing the default connection of the Dallas Branch to MODEM.

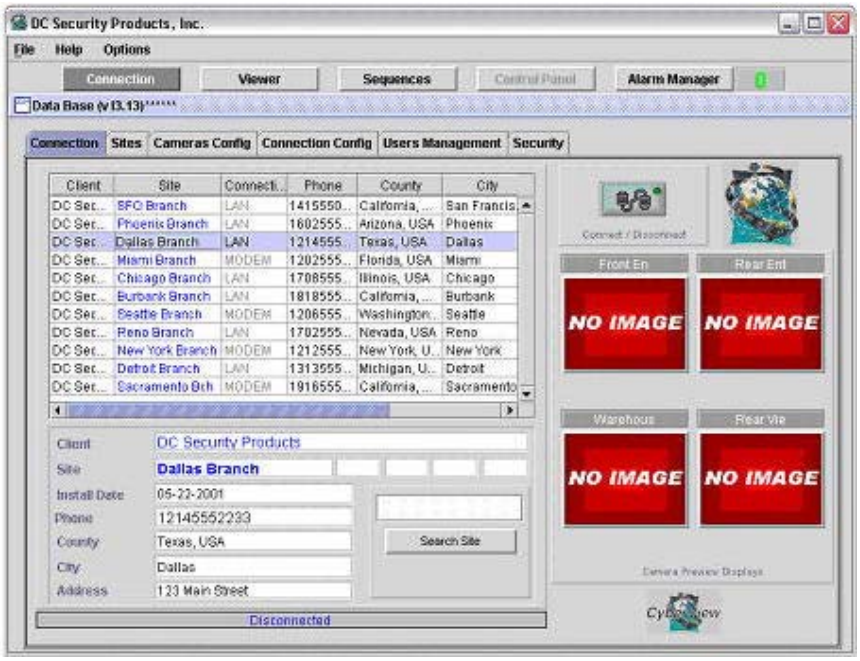


FIGURE 30. CONNECTION SCREEN DISPLAYING THE LAN CIRCUIT

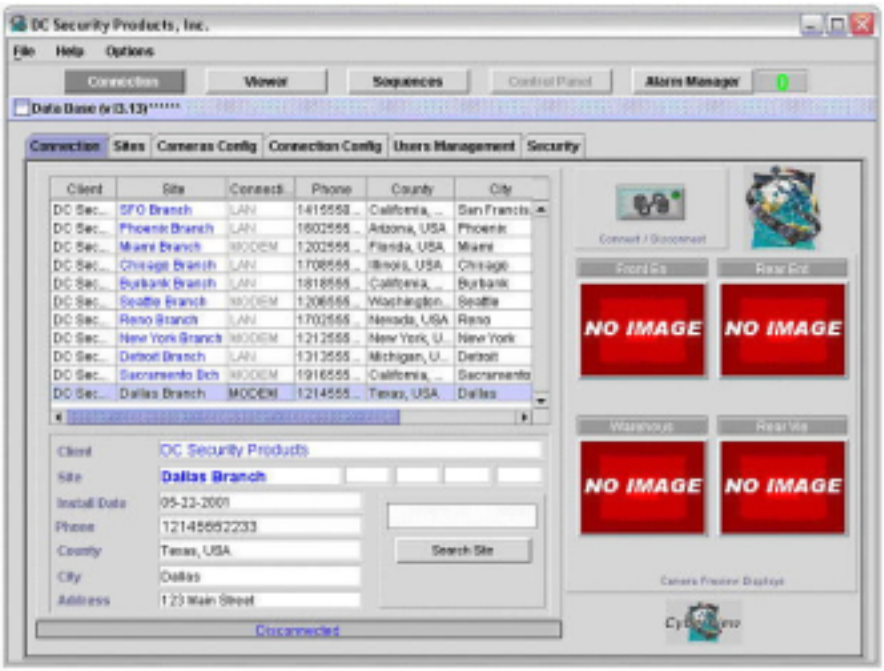


FIGURE 31. CONNECTION SCREEN DISPLAYING THE NEW MODEM CIRCUIT

Chapter 5
Sample Customer Installation Introduction

In this chapter, an IPTV system (the *CyberStation*™ Controller and the host PC containing the *CyberView*™ Software Suite) will be fully configured. The customer requirements introduced are found in many real world, small business situations. Throughout this chapter all required *CyberStation*™ system parameters are configured and the systems are readied for operation. Installers are encouraged to use these real world parameters and values.

5.1 Sample practical example

This example consists of a *CyberStation*™ Controller located on customer premises, which is a bank branch sales office. The *CyberStation*™ provides the following functions:

- records video from the various cameras, depending on branch time tables (working times) and on the state of several sensors.
- will send alarms (with and without associated video pictures), according to branch time tables, and on the state of several detection device sensors.
- Supplys services for external PSTN calls that, in turn, provides transmission of recorded or real time video.

The System also utilizes *CyberView™, the Video and Alarm Management Software* to:

- receive dispatch and qualify alarms.
- perform surveillance of the branch and display requested video, recorded in the *CyberStation*™ Controller's hard drive.

5.1.1 Security elements installed in the Dallas Branch

The *CyberStation*™ is installed in a bank branch office identified as `Dallas Branch`. It has two rooms:

- **Room 1**—contains security safes to hold customer valuables. Installed is a motion sensor, "safes-room-IR". Its logical value is activated (TRUE) whenever a moving person is in the room. The camera is named, "cust-safes-cam".

- **Room 2**—is where customers are attended. There is an alarm panel, a camera named "main-cam" and motion detector, "office-IR". "Office-move" is TRUE whenever a person is moving in the room. A switch in the alarm panel tracks the alarm panel's armed/disarmed status. The security manager is responsible for arming/disarming the alarm panel for branch security, when the office opens in the morning and closes at the end of the day. Another camera, identified as, "branch-safe-cam", points to the branch office main Safe. There is also an exterior sounder.

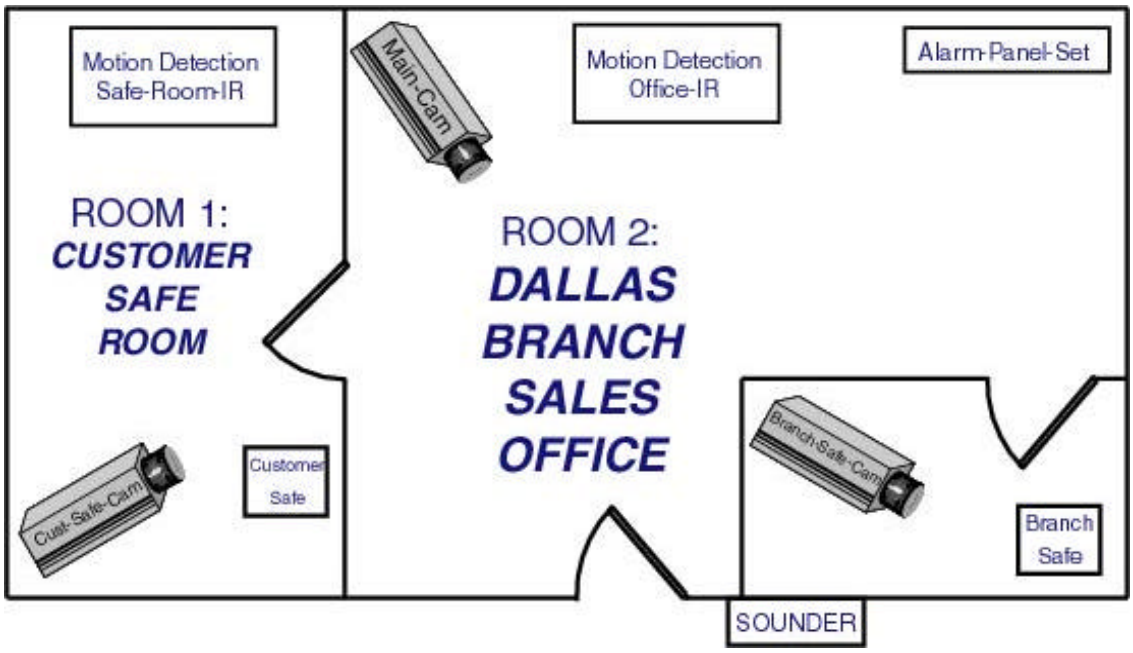


FIGURE 32 . SECURITY ELEMENTS IN DALLAS BRANCH OFFICE

5.1.2 Video recording

Video from the cameras is recorded in the *CyberStation*'s hard drive, according to the required criteria for each individual camera.

5.1.2.1 "Cust-safes-cam" camera

Video recording in this camera is event driven and dependant upon the state of the motion detection sensor "safes-room-IR". The recording pattern is as follows:

- 10 minutes prior motion sensor activation (pre-alarm) at 2 images per second (ips).
- 1 minute when event happens (alarm) at 3 ips.
- 5 minutes after motion sensor resets (post-alarm) at 2 ips.

Activation of the motion detection sensor "safes-room-IR" does not cause an alarm to be transmitted to the *CyberView*™.

5.1.2.2 “Branch-safe-cam” camera

Video recording in this camera is time state driven, dependant on time state schedules. Recording is during work hours, when the Branch Safe is open. The Safe remains open one hour, but the opening time depends on the season, changing from Summer to Winter.

5.1.2.3 “Main-cam” Camera

Video recording in this camera is both event and time state driven, and is dependant on the operational state of the alarm panel. The possible states are: “cleared” or "disarmed", during working hours or "armed" the rest of the time. The security manager is responsible for arming and disarming the alarm panel. When the alarm panel is cleared, recording is continuous (one phase) at 2 ips. When the alarm panel is set without employees in the office, recording depends on the motion sensor, “office-IR,” status. It is event driven and recording patterns are as follows:

- 5 minutes prior sensor activation (pre-alarm) at 2 ips.
- 1 minute on sensor activation (alarm), at 3 ips and.
- 5 minutes after (post-alarm) at 2 ips.

In addition, when the sensor, “office-IR,” is activated, it sends an alarm to *CyberView*™.

5.1.3 Generation of alarms

The *CyberStation*™ in Dallas Branch generates alarms both with and without video pictures. Alarms are sent to the host management program, comprised of a PC equipped with an analog modem and the *CyberView*™ application, properly installed and operating.

5.1.3.1 System alarms (alarm without video)

Alarms without video are issued if one of the following events occurs:

- **Disk full.** The bank should ensure that the *CyberStation*™ will record video during periods of time equal to or longer than 15 days. The *CyberStation*™ issues this alarm to the receiver if the disk capacity is insufficient to record for 15 days. At alarm receipt, the operators may decide what to do.
- **Disk not available.** If for any reason the disk is not ready to record, as far as the *CyberStation*™ is concerned.
- **Alarm panel set or "Armed".** The *CyberView*™*,* PC side, must be advised that the alarm panel is set/clear at due time and react otherwise.

5.1.3.2 General alarms (alarms with video)

Based on our programming, alarms that trigger video images are transmitted only when the events “alarm-panel-set” (i.e., armed) and “office-IR” (i.e., someone has tripped the IR) are both TRUE (i.e., both activities need to take place before an alarm is triggered and video picture is sent). These conditions can occur when the “main-cam” camera recording is done (because the person could have violated this area first), based on the event transmitted by “office-IR”.

While the alarm panel is set, if someone is moving in the office, “office-IR” is activated (TRUE), video from the main-cam camera is recording, the external sounder is activated, and an alarm, including a video picture, is sent to the *CyberView*™.

5.1.4 Communications

The *CyberStation*™ uses the LAN network to communicate to *CyberView*™ receiver and the PSTN network to communicate to mobile PCs using Securcomm modems.

The *CyberView*™ receiver may display real time or recorded video at operator command. The LAN calls are placed from the receiver. It may also receive alarms sent from the controller. In this case, the LAN calls are placed by the *CyberStation*™. The PSTN calls, either inbound or outbound, use analog circuits.

At select times, the security manager may wish to perform remote surveillance, watching real time video from his portable PC while he is out of the office. To accept calls from his PC, the Uniflex modem module is installed in *CyberStation*™ and connected to the PSTN network. In the portable PC, the required software is *CyberView*™, with a compatible modem installed.

5.1.5 Timetable Dallas Branch

There are two timetables in the office, depending on the dates, referred to as Summer timetable and Winter timetable.

Within a specific timetable, three time states are defined for the operation of the *CyberStation*™,. The time states specify the orders to record video or to send alarms.

- Diurnal (Daily/Normal) time-state when the office is open. From 0900 to 1400 and from 1600 to 2000 in winter and from 0800 to 1500 in summer. Winter extends from January 1 to June 15 and from September 15 to December 31. Summer extends from June 16 to September 14. This applies to no holiday weekdays Monday to Friday.
- Night time-state is when the office is closed. It is the hours of the day not defined as Diurnal, Saturdays, Sundays and holidays.

- The Special time-state is when the branch Safe is open. These hours are from 1400 to 1500 in summer time table and from 1300 to 1400 in winter timetable.

January 1, May 1 and December 15 are specified as holidays.

5.1.6 Configuration process review

There are several essential elements required for a full configuration of an IPTV system. They are:

- the *CyberStation*™ controller
- the *CyberView*™ application

The following application utilities contained in the PC host's Windows® operating system are utilized by the *CyberView*™ Software Suite:

- dial-up networking
- Remote Access Server

Figure 33 through Figure 35 display the necessary values to help identify the hypothetical configuration parameter values. In an actual situation, the user provides those values to the installer. The Figures highlight (in order):

- General Overview: cameras, inputs, outputs, communication ports and circuits
- IP addresses and phone numbers involved in the configuration of circuits
- Username and Passwords of the circuits

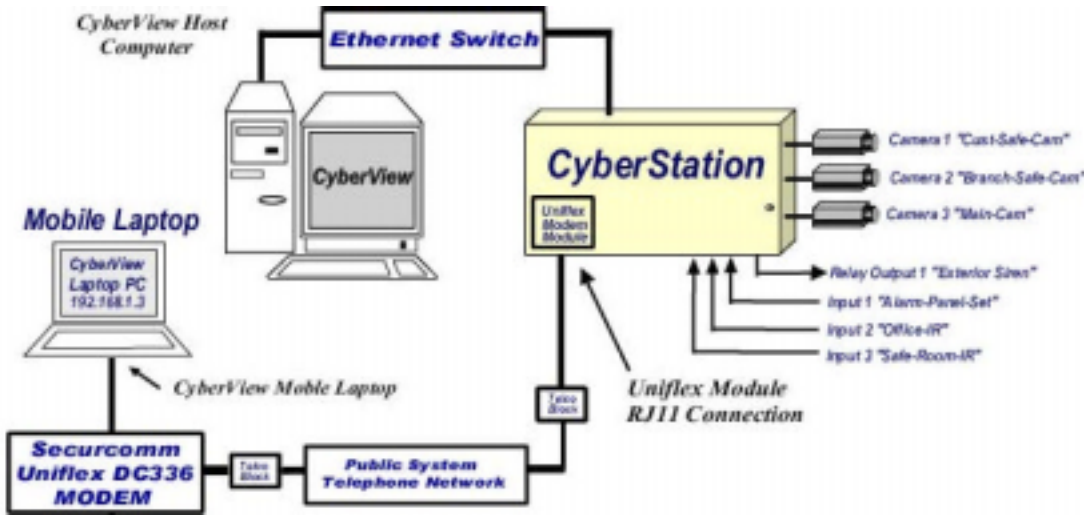


FIGURE 33. SAMPLE CONFIGURATION GENERAL OVERVIEW

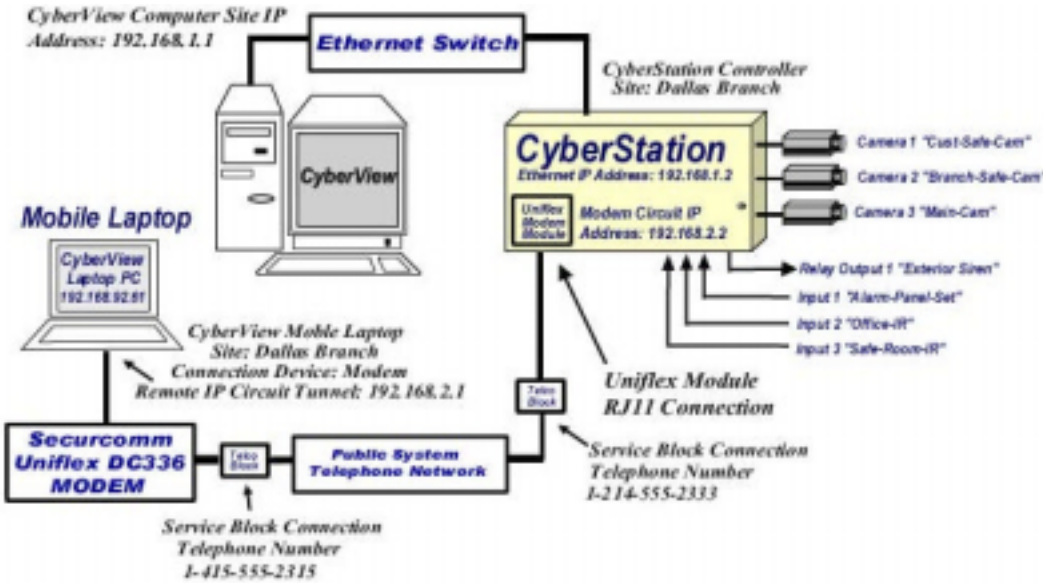


FIGURE 34. CIRCUITS : IP ADDRESSES AND TELEPHONE NUMBERS

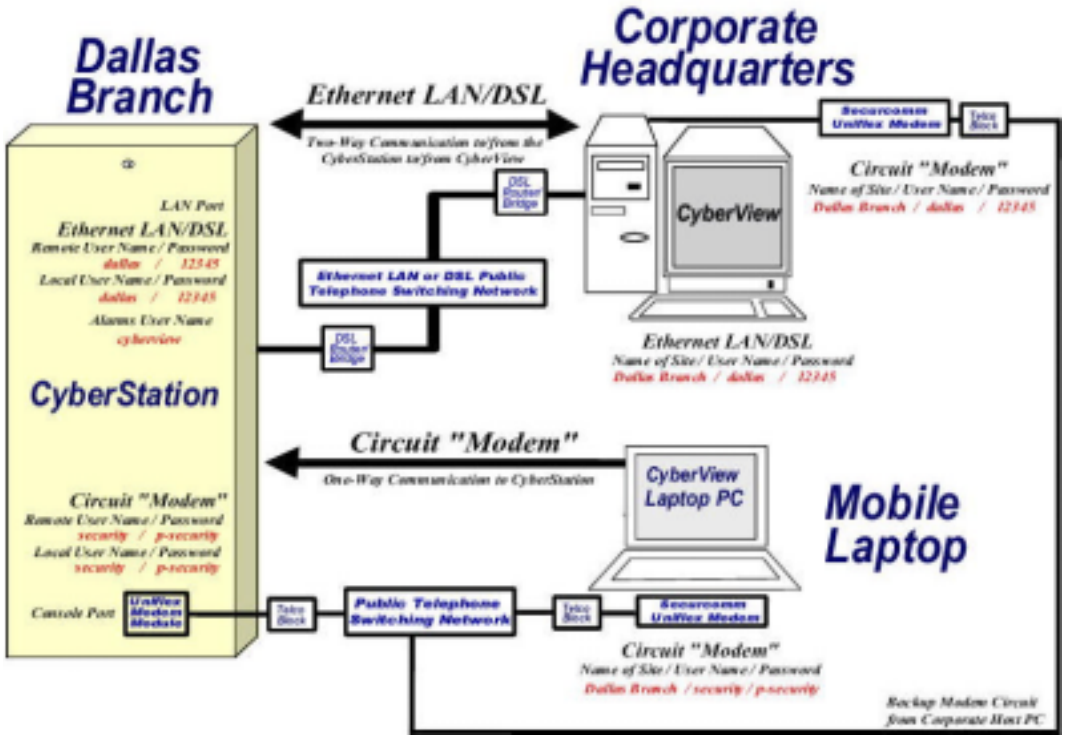


FIGURE 35. CIRCUITS: USERNAMES / PASSWORDS

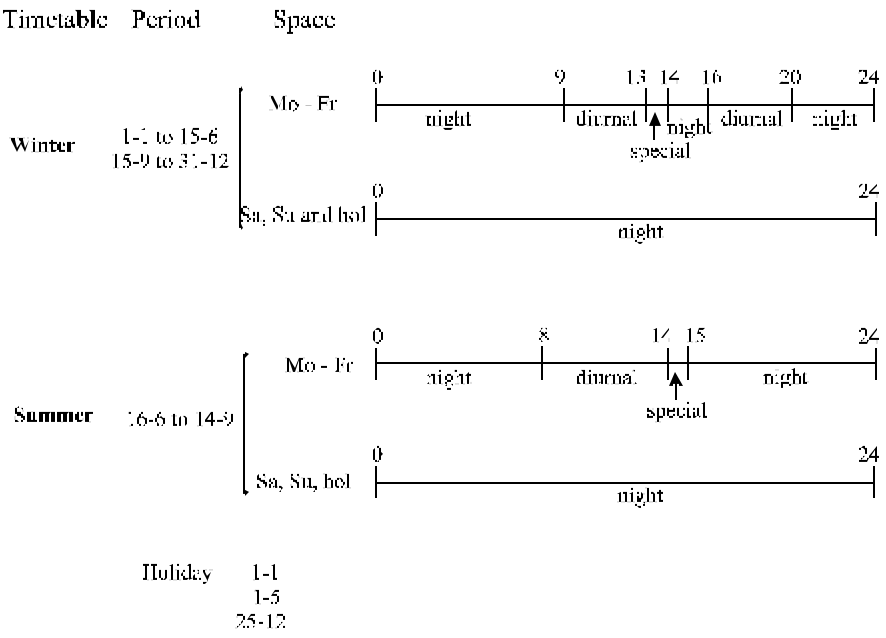
The other values are displayed in the *CyberStation*™ Users information table below:

CyberStation™ Users information:

Users	Password	Applications	Description
Dallas	12345	ppp-server images	The receiver can place a call to connect to *CyberStation*™ to display video at operator command.
CyberView™	12345	ppp-client images	The *CyberStation*™ may place a call to the receiver in case of alarms, including video pictures if required.
Security	p-security	web ppp-server images	May view real time video accessing the controller from an Internet browser. May control moving cameras.
CyberStation™	*CyberStation*™	All	*

(*) Usually, every system requires a user with privilege to access all *CyberStation*™ applications, to manage and change the configuration if necessary. In our example, this user is *CyberStation*™.

Timetable information:



Inputs/Outputs information:

Input	In1	Alarm-panel
	In2	office-IR
	In3	safes-room-IR
Output	relay1	Sounder

Alarms without video information:

Center name	Dallas Branch	*
Username	Dallas	*
IP of *CyberView*™	192.168.1.1	
Retries number	3	
Saved days	15	
System alarms	Disk full	
	Disk fault	
Other alarms	Alarm panel set	If alarm-panel
	Alarm panel clear	If not alarm-panel

(*) Parameters must be configured in *CyberView*™.

Video information:

Camera	Description	Recording conditions
camera 1	"cust-safes-cam"	Records on "safes-room-IR"(event driven, no alarm sent) pre-alarm / alarm / post-alarm Recording time: 10 min / 1 min / 5 min Recording speed: 2 ips / 3 ips / 2 ips
camera 2	"Branch-safe-cam"	Scheduled recording on Special time-state. Records continuously, at 2 ips when time-state is Special.
camera 3	"main-cam"	Records in two different ways: - If the Alarm-panel is armed (office closed) when "office-mov" (by event, sends alarm with video picture) pre-alarm / alarm / post-alarm Recording time: 5 min / 1 min / 5 min Recording speed: 2 ips / 3 ips / 2 ips Activate sounder - If Not Alarm-panel (Diurnal Timetable) it records continuously at 2 ips.

Circuits:

Circuit	Interface	Specifications	
Moble laptop	Serial-1 (modem)	security p-security 192.168.2.2 192.168.2.1	Remote username local ip remote ip

Modem information:

Interface	Specifications	
serial-1 (*)	Protocol [modem-ppp] baud-rate [38400] flow-control [Hardware] dial-string [ATDT] hang-up string [ATH0] answer-string [AT&F&D3X2M0S7=60S0=1&W0]	Protocol speed flow-control dial-string hang-up string answer-string (**)

(*) The modem should be in the multi-protocol serial port (serial-1 in the configuration. For additional information, refer to the *CyberStation*™ Reference Manual, Section 4.5.2.1, Configuring serial-0 and serial-1 for modem).

(**) AT modem commands used for a standard Securcomm Uniflex Modem. For information on additional modem models, refer to the *CyberStation*™ Reference Manual, Section 4.5.3.1, Modem configuration).

Hardware information:

Module	Specifications
CommPort232 (Serial-1)	The optional CommPort232 module allows you to connect the modem in the multi-protocol serial port.
Securcomm Uniflex DC336B	The optional Uniflex module allows you to connect the modem in the PSTN.

To connect the Uniflex modem module to the multi-protocol serial port, the optional CommPort232 module is required (this is an optional accessory module and is NOT included with the *CyberStation*™ base package).

5.2 Dallas Branch Configuration file

The configuration file is fully displayed in Section 5.1 Sample practical example, and is shown below:

```
users
  user name dallas password *****
    level administrator
    apps pppserver+images
  user name CyberView password ***********
    level administrator
    apps pppclient+images
  user name security password ********
    level user
    apps pppserver+web+images
  user name CyberStation password ******
    level administrator
    apps telnet+pppclient+pppserver+ftp+web+console+images+configuration+
email

timetable
  holiday 1-1
  holiday 1-5
  holiday 25-12
  name Winter
    period from 1-1 to 15-6
    period from 15-9 to 31-12
    interval from 0:00 to 9:00
      time-state night
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 13:00 to 14:00
      time-state especial
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 14:00 to 16:00
      time-state night
      week-days monday+tuesday+wednesday+thursday+friday
  interval from 20:00 to 24:00
      time-state night
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 0:00 to 24:00
      time-state night
      week-days sunday+saturday+holiday

  name Summer
    period from 16-6 to 14-9
    interval from 0:00 to 8:00
      time-state night
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 14:00 to 15:00
```

```
      time-state special
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 15:00 to 24:00
      time-state night
      week-days monday+tuesday+wednesday+thursday+friday
    interval from 0:00 to 24:00
      time-state night
      week-days sunday+monday+holiday
io
  input name in1 description alarm-panel-set
  input name in2 description office-IR
  input name in3 description safes-room-IR
  output name relay1 description sounder

alarms
  site-name "dallas branch"
  username dallas
  ip 192.168.1.1
  retries 3
  saved-days 15
  system-alarms hd_failure+hd_full
  message "Alarm panel set"
    time-state diurnal+night+holiday
    event description "Alarm panel  set" function alarm-panel-set
    send-alarm yes
  message "Panel alarms disable"
    time-state diurnal+night+holiday
    event description "Alarm panel disabled" function not.alarm-panel-set
    send-alarm yes

video
  standard NTSC
  camera 1
    description cust-safes-cam
    recorder "Motion in safes room"
      time-state diurnal+night+holiday+special
      event description "You detect motion" function safes_room_mov
      time before 600 on 60 after 300
      rate before 2 on 3 after 2

camera 2
    description branch-safe-cam
    recorder "Opening the safe"
      time-state special
      time before 0 on 0 after 0
      rate before 1 on 1 after 1
```

```
  camera 3
    description general
    recorder "working hour"
      time-state diurnal+night+holiday+special
      time-event description "Alarm panel disabled" function not.alarm-panel-set
      time before 0 on 0 after 0
      rate before 1 on 2 after 1
    recorder "no working hour"
      time-state diurnal+night+holiday+special
      time-event description "Alarm panel set" function alarm-panel-set
      event description "Motion detected" function office-IR
      time before 300 on 60 after 300
      rate before 2 on 3 after 2
      send-alarm yes
      outputs sounder

circuits
  circuit Modem
    interface serial-1
    auth-type pap+chap
    remote-username security-manager
    ip address 192.168.2.2 mask 255.255.255.0
    remote-ip address 192.168.2.1
    call-type accept

circuitcontrol
  multilink active no

ethernet
 mac address 0009D7:900019
  ip address 192.168.1.2

serial
  interface serial-1
    protocol modem-ppp
    baud-rate 38400
    flow-control hardware

modem
  interface serial-1
    dial-string ATDT
    hangup-string ATH0
    answer-string AT&F&D3X2M0S7=60S0=1&W0

hardware
  modules SERIAL-1
```

5.3 Installing the Cyberstation™

This section briefly describesthe installation of the *CyberStation*™ in its tamper-resistant cabinet. First, open the cabinet to access the connectors and boards. The cabinet has mounting holes equally located 16” apart and can be wall-mounted horizontally or vertically. There are slot openings to run the wire and cable as well as two 2” knockouts and two 1” knockouts for conduit piping. To access the connectors and boards within the cabinet, unlock it, using the keys supplied. The cabinet is depicted in Figure 36.

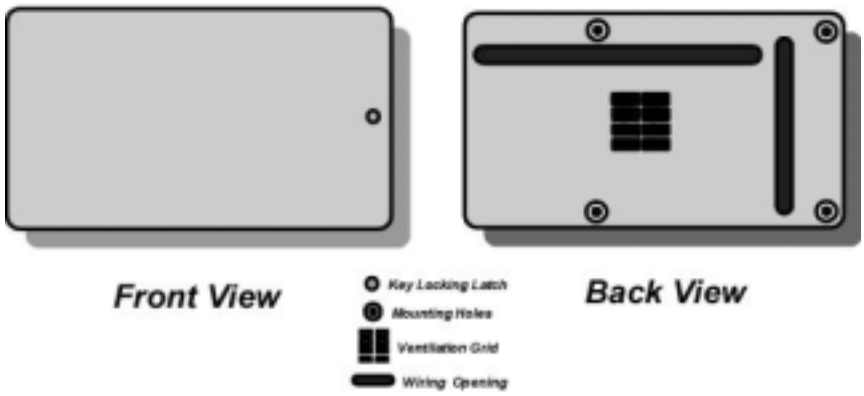


FIGURE 36. VIEWS OF THE *CYBERSTATION*™ ENCLOSURE

The ***CS4431AHD*** main board is installed in the *CyberStation*™ cabinet. Cameras and sensors are attached to the board, as shown in Figure 36.

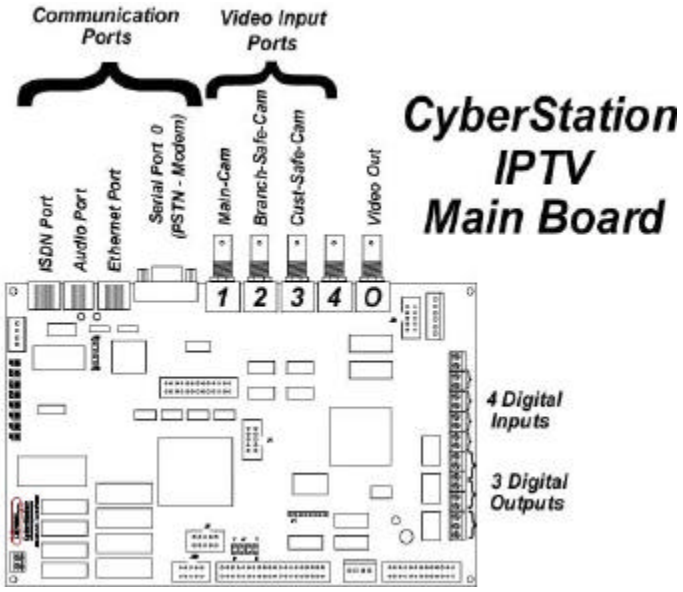


FIGURE 37. *CYBERSTATION*™ CONTROLLER MAIN BOARD LAYOUT

The Digital Inputs are activated by the opening/closing of a connected sensor or contact. Usually, they are opened. When they are closed (connection with ground signal) an alarm condition is caused. The output relay is an open/closed relay, without polarity.

FIGURE 38. CONTROLLER'S INPUT AND OUTPUT LEADS

CyberStation™ Reference Manual, Appendix III, contains more detailed information about all available models.

5.4 Configuring the *CyberView*™ Software Suite

In our Dallas Branch example, the *CyberView*™ has two functions: the first allows the operator to watch real time or recorded video by placing phone calls; the second receives phone calls placed by the *CyberStation*™ in case of alarms. In the following paragraphs, we describe both the *CyberView*™ and Windows® configuration for optimal performance. Also, note that calls may be received by a properly configured modem supporting dial-up ppp.

The operating system described is Windows® 98/XP. Users may find the corresponding information about Windows® NT/2000 in their Microsoft® documentation. The *CyberView*™ Reference Manual describes how to configure a Windows® NT/2000 system as a PC Host.

5.4.1 Configurating to call the Controller

The configuration procedure is explained in Sections 4.4 and 4.5 . Please review the procedures to configure *CyberView*™ and to access the *CyberStation*™ using Modems.

5.4.2 Configuring *CyberView*™ to receive alarms

To manage the communications with the *CyberStation*™, *CyberView*™ uses communication utilities available in the Windows® 98 Operating System, Dial-up networking (DUN) to place calls and the Dial Up Server (DUS) to receive calls.

A PPP circuit is configured between *CyberStation*™ and *CyberView*™ for one POTS call. Either end, *CyberStation*™ *or* Windows® *XP*/*98*/*95* can place calls, according to PPP or MLP. The caller acts as a PPP client and the receiver as a PPP server.

To place calls, The DUN configuration is perfomed automatically when the Controller is configured in *CyberView*™, as described in Section 4.5.

To receive alarms, the DUN must be configured as described in Section 5.4.4 Configure the DUN utility in the .

5.4.3 Configuring the Dial-Up Server in W98

To configure the W98 PC to accept calls:

1. Configure TCP/IP of the PC
   a. Select Start >Control Panel->Network->Configuration.
   b. Select TCP/IP->Dial-Up Adapter.
   c. Click **Properties**.
   d. In the IP Address tab Select ⊙ in **Specify an IP address** and enter the same IP address used in *CyberStation*™
   e. In the field **remote-ip** in the context circuits (in our example *192.168.1.2*). Enter the address mask (for this example 255.255.255.0).
2. Configure the Dial-Up Server
   a. Select: Start>Programs->Accessories->Communications->Dial-Up Networking-> Connections->Dial-Up Server >. Select the suitable tab.
   b. Set the radio button ⊙ in Allow caller access.
   c. Click Change Password....
   d. The password must be the same as assigned to the *CyberStation*™ user in the field “local-username” within the “Circuits” context (in our example p-receiver).

e. Click Server Type . Select PPP, disable ☐ Enable software compression and enable ☑ Require encrypted password .

f. Click OK then Apply.

If the steps are performed successfully, the word `Supervising` appears in the in the State or Status field.

5.4.4 Configuring the Dial-Up Server in Windows® *NT*

1. Install the Dial-Up Server.
2. Select `Start>Control Panel->Add/Remove Programs -> Windows Setup->Communications->Details`.
3. Mark with ☑ the **`Dial-Up Server`** .

   To Configure the Dial-Up Server:

   a. Select `Control Panel->Network`. Select the Services tab.

   b. Select `Dial-Up Server`.

   c. Click Properties, and select the device.

   d. Click To configure... .

   e. In `Port use`, click the **`To make and to receive calls`** radio button.

   f. Click Network.

   g. In Protocols to make calls: select ☑ TCP/IP , disable ☐ the other protocols.

      a. In `Server configuration`:
         - **`NetBEUI`** , **`IPX`** disable ☐.
         - Select ⊙ **`To allow any authentication type, even plane text`**.
         - Select ☑ **`TCP/IP`** ,and click in **`To configure…`**:
           - Enable ⊙ in `To allow remote TCP/IP clients access to`: **`All the network`** or **`Only this system`**, as you wish.

- Disable ○ **Use DHCP for allocating address to remote TCP/IP clients**.
- Enable ⊙ **Use the address static group**:
  - **Begin** IP1 **to** IP2. The WNT use the first IP address (IP1) as his own and the rest are IP address allowed for remote users. For example, configure **Begin** 192.168.1.1 **to** 192.168.1.10. The *CyberStation*™ should use IP address between 192.168.1.11 and 192.168.1.254, not included in the first range defined but in the same network (in the *CyberStation*™ the masque 255.255.255.0 is programmed).

- Select ☑ **To allow remote client to ask for an specific IP address** .

4. Configure the Dial-Up server as automatic:

   a. In Control panel->Services, select Dial-Up Server and double click. In Start type enable ⊙ **Automatic**.

   b. Create a user:

   - **In** Start->Programs->System tools-> User manager. Select the menu User->New user
   - Type the **User name** and the **Password**.
   - Disable ☐ **The user should change the password in the following start session**.
   - Enable ☑ **The password never expires**.
   - Disable ☐ **Account disable**.
   - Click on **Dial**:
     - Enable ☑ **To enable user to call.**
     - In Answer, enable ⊙ Not answer.

View the state of connection in:

Start->Programs->System tools a->Dial-Up manager:

If the call is established, you can disconnect it.

5.4.5 Configuring the Dial-Up Server in Windows® *XP*

1. Select `Control panel-> Network connections and Internet->Network connections.`

   a. Select in `Network task and` **`Create a new connection`** and next, click on **`Next >.`**

   b. Click ⊙ in **`To configure an advanced connection`**, and **`Next >`**.

   c. Click ⊙ in **`To accept incoming connections`**, click in **`Next >`** and follows the new connection assistant

2. In `Control panel-> Network connections and Internet-> Network connections.`

   a. Select in `Network task, Change the configuration of this connection.` In the tab `Network functions`, click ⊙ in **`Internet Protocol (TCP/IP)`** , and next, in **`Properties ...`**

   b. Click ⊙ in **`Specify TCP/IP address`** and then:

3. In **`From`**, write the start IP address. (For example, *`192.168.1.2`*)

4. In **`To`**, write the final IP address. (For example, *`192.168.1.3`*)

5. Enable ☑ **`To allow to the system which calls to specify its own IP address`** .

5.5 Configuring the portable PC to access *CyberStation*™ controller using Internet Browsers

As previously indicated, users are required to access the *CyberStation*™ not only from *CyberView*™, but also from an Internet browser with a portable PC with Windows® 98 and a modem.

The calls from the portable are performed using the Microsoft® DUN utility available in Windows® XP/98.

5.5.1 Phone numbers

According to values used in our example (Figure 34 and Figure 39), the *CyberStation*™ Controller has an installed Uniflex modem module plugged to serial-1 and connected to the PSTN network. The phone number is 12145552333.

5.5.2 Username and password

Users (and application access) must have a username and a password to access *CyberStation*™. There are various user access available in the configuration. Limited access by using: Username: **security** Password: **p-security** as well as user profiles with full access as described in Section 5.1.6 .

5.5.3 PC modem installation – Step-by-step procedure

Ensure that a PC with a properly configured modem adapter is available.

1. Configure the DUN utility in the PC (ask the information system or network administrator if you are in doubt). In fact, the configuration to connect the PC to Internet using a dial up network, but with different phone number, username and password.

2. Place the phone call. Wait for the connection to be established.

3. Launch the browser, if not previously done.

4. Type in the required IP Address URL in the browser. Wait until the Java Applet (or the Javascript) is downloaded from *CyberStation*™ and starts. View the cameras at will.

5. To finish, close the phone call using DUN to disconnect from *CyberStation*™.

5.5.4 Configure the DUN utility in the PC

Assign the configuration values as indicated.

Phone number and Controller selection:

1. Select `Start->Programs->Accesories-> Communications->Dial Up Networking` and click on `New connection`, assigning a name to the connection (for instance, *demo_CyberStation™*). The user must select the available modem, previously installed in Windows® 98 following the manufacturer instructions.

2. Select the device and type in **Next.**

3. Type the **Phone number**, in our example: *963302438*.
4. Right-click on the new DialUp Networking icon, *demo_CyberStation*.
5. Select "Server setting".

5.5.5 Server setting

The connection between the PC and the *CyberStation*™ uses the Internet protocol PPP, with the *CyberStation*™ as the server, while the PC with DUN is the client. All advanced options in the Server setting form must be cleared, as well as NetBEUI and Compatible with IPX/SPX. The protocol selected must be TCP/IP.

For TCP/IP configuration:

Click in **TCP/IP configuration** and configure the parameters as follows:

- IP address assigned by the server.... "set".
- DNS addresses assigned by the server.... "set".
- Use IP header compression.... "clear".
- Use the preset link port in the remote network...."set".

5.5.6 Place the phone call

If properly configured, clicking on the new DUN icon launches the login screen. Type the username (security), the password (p-security) and the phone number (12145552333).

Clicking **Connect** sets-up the call. It is an authenticated ppp call. If the procedure proceeds properly, Windows® will display an icon in the bottom-right corner of the screen, consisting of a pair of PCs. The call may fail for several reasons, for instance, the phone line being busy if the call does fail, recheck settings and try again. Once connected the PC is now on-line with the *CyberStation*™ and may launch the browser.

5.5.7 Accessing *Cyberstation*™ embedded web pages

Once the phone connection is complete, and the *CyberStation*™ is connected, the user is ready to download images through the embedded web pages that allow viewing via your browser. Once connected, open a browser and in the **Location** field (if Netscape) or in the **Address** field (if Internet Explorer), type the desired URL in the following format:

URL: **http://*(CyberStation-ip-address)*/*web_page_name***

In the URL field, users must type the name of the web page to download. The use of each of the *CyberStation*™ web pages is explained in detail in the *CyberStation*™ Reference Manual.

***CyberStation*™ Embedded Web-Pages**
webcam.html
webcctv.html
camera.html
displayer.html
netsc_pushcam
netsc_pushcamx2
ronda.html
motion.html
sequences.html

5.5.8 CyberStation-ip-address

In keeping with the example described in Chapter 5, the function of the IP addresses set to the PSTN circuits in Figure 34 and the IP address set to the Ethernet interface in Figure 33, the URLs to enter in the Browser to obtain the web page **webcam.html** are:

- LAN connection:
  - (CyberStation-ip-address)= 192.168.1.2
  - URL= http://192.168.1.2/webcam.html

- PSTN modem connection
  - (CyberStation-ip-address)= 192.168.2.2
  - URL= http://192.168.2.2/webcam.html

While viewing images in Internet Explorer from the various *CyberStation*™ Hypertext screens, a number of “Stack Overflow” error messages can appear (as shown below).

FIGURE 40: STACK OVERFLOW ERROR MESSAGE

To avoid this streaming error, and to have uninterrupted viewing from the *CyberStation*™ in real time via browser, configure your version of MS Internet Explorer.

1. Open Internet Explorer.
2. Select `Tools->Internet Options.`
3. Select `Internet temporary files, Configuration...` or `Settings...` (depending on the version of Internet Explorer you are using).
4. In the panel,”`Check if there are new versions of the stored web pages`”, click the radio button ⊙ corresponding to ⊙ **`Every time you visit the web page.`**
5. Once this procedure is completed the error should cease.