# Crestron **e-Control**®

# Reference Guide

CRESTRON

This document was prepared and written by the Technical Documentation department at:

CRESTRON™

Crestron Electronics, Inc.
15 Volvo Drive
Rockleigh, NJ 07647
1-888-CRESTRON

# Contents

# Crestron e-Control®

## Introduction

Crestron e-Control® is a broad-based technology that integrates Crestron audio/visual control into Ethernet/IP networks. Ethernet technology has been used since the mid 1970s and is the most widely accepted standard throughout the world. By using Ethernet in your control applications, you are following the common trend in technology today. In addition, you gain the ability to harness the speed and flexibility of the Internet to access, analyze, and diagnose control system functions.

Crestron e-Control offers many benefits, including:

- Worldwide acceptance of Ethernet products and use of standard networking protocols.
- Ability to use low-cost Ethernet switches and other affordable Ethernet physical media.
- Connections that are simple to wire, and easy to debug and maintain.
- Support for both 10 and 100Mbps products and half and full-duplex transmission.
- Support for static and dynamic IP addressing.
- Control systems with built-in Web server capability, allowing devices to be controlled using a standard Web browser.
- Analysis, control, and diagnostics available at any time or place.

This document is your reference guide to e-Control. The first half reviews the basic networking principles needed to set up and maintain an e-Control network. This includes an explanation of common networking terminology as well as cabling specifications and concepts such as static and dynamic IP addressing, subnet masks, and port numbers. The second half deals with specific e-Control applications, including hardware setup and configuration, software programming, and system-to-system communication.

This electronic document will continue to be updated as Crestron adds new features and capabilities to e-Control, so be sure to check back for the latest information.

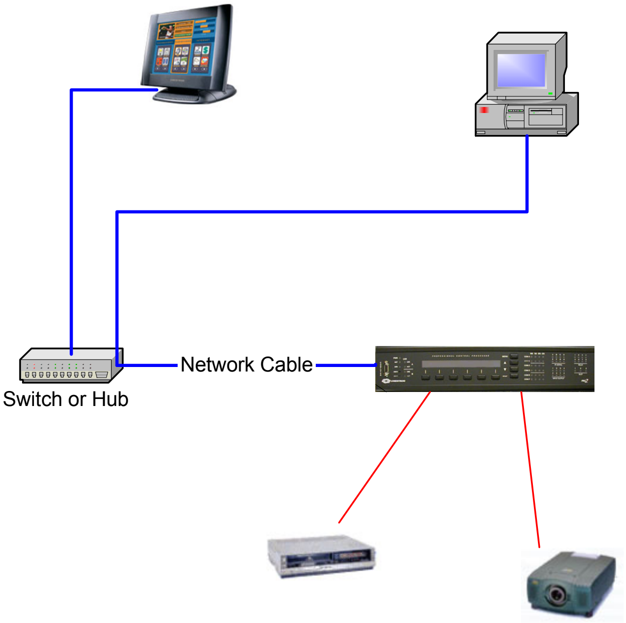
# Ethernet Networking

**NOTE:** This section reviews basic Ethernet and IP networking principles that form the foundation for e-Control. Even if you are familiar with these terms or have prior networking experience, the material contained here will help you better understand how Crestron implements e-Control. You can also refer to “Appendix A: Glossary” on page 46 for a list of networking terms and acronyms used throughout this guide.

A **network** is any collection of independent computers, printers, and peripheral devices that are connected by cables. A network incorporating e-Control will also typically include connected Crestron control systems, network control modules, and touchpanels that control AV, lighting, and other equipment. Information travels over the cables, allowing users on the network to communicate, exchange data, and control equipment. Each device that is connected to the network is called a **node**. Networks can have tens, thousands, or even millions of nodes.

**L**ocal **A**rea **N**etworks (**LAN**s) are usually confined to a geographic area, such as a single building or a college campus. LANs can be small, linking as few as two or three computers, but often can link hundreds of computers used by thousands of people. **W**ide **A**rea **N**etworks (**WAN**s) such as the Internet combine multiple LANs that are geographically separate.

The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations. The most popular LAN technology in use today, and the standard that is the basis for e-Control, is **Ethernet**, which consists of computers and devices cabled together according to specific rules defined by the Institute for Electrical and Electronic Engineers (IEEE).



Ethernet networks are categorized by how fast they can transfer data. Speed is expressed in **m**ega**b**its **p**er **s**econd (**Mbps**) and even **g**iga**b**its **p**er **s**econd (**Gbps**). One "bit" is equal to 1/8th of a character, letter, or number. **Standard Ethernet** operates at 10Mbps, which is fast enough for most networking tasks. Crestron’s X-Series control systems and CEN devices operate at 10Mbps. **Fast Ethernet**, by contrast, operates 10 times faster at 100Mbps, making it ideal for video, multimedia, and other speed-intensive applications. Crestron’s 2-Series control systems and TPS Ethernet-enabled touchpanels can operate at 10Mbps or 100Mbps. Fast Ethernet and Standard Ethernet are not readily compatible; making the two speeds communicate on the same network requires special equipment such as a switch.

Some network devices, including Crestron 2-Series control systems and TPS Ethernet-enabled touchpanels, can determine the speed of data transfer and automatically adjust to that speed. This is called **auto-sensing**. Any device that has been labeled “10/100” or “auto-sensing” should be able to work with any standard Ethernet network devices, regardless of speed, provided that the proper cabling is used.

**Full duplex** and **half duplex** are terms that refer to how data is transferred over a network. Duplex means "two-way", and describes the sending and receiving of data. If a device is full duplex, it means that the device sends and receives data simultaneously. If it is a half duplex device, it alternates between sending and receiving. Thus, a 100Mbps full duplex device (such as a Crestron 2-Series control system or TPS Ethernet touchpanel) is actually operating at 200Mbps. A 10Mbps half duplex device (such as a Crestron X-Series control system or CEN device), alternates between sending at 10Mbps and then receiving at 10Mbps.

## Network Cards

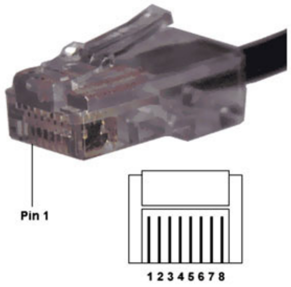
To communicate over Ethernet a device must have an Ethernet network card or adapter installed. Ethernet network cards (often called **N**etwork **I**nterface **C**ards, or NICs) are installed inside a device, while network adapters are external. Some Crestron control systems, such as the MP2E, come with an Ethernet network card already built in, whereas others like the PRO2 require separate purchase of a C2ENET card (shown in the figure). TPS touchpanels connect to the Ethernet network via a Crestron TPS-ENET or a TPS-ENETL card.

Ethernet networking also requires at least one hub or switch to act as the central point of the network. This is because you can’t string multiple devices on an Ethernet network directly into one another. They must connect at a central point. (However, a crossover cable can be used when connecting only two devices together.)

## Cables, Hubs, and Switches

Special cabling is required to build an Ethernet network. One end of an RJ-45 cable plugs directly into the device’s Ethernet network card or adapter, and the other end plugs into a switch, hub, or similar device, connecting that device to the other networked devices.

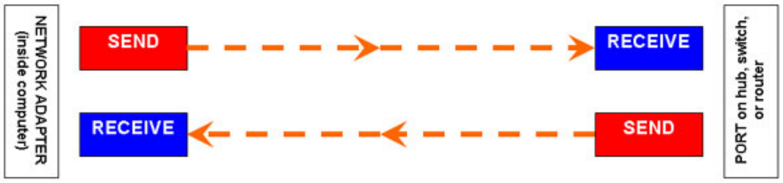
**RJ-45** connectors look like standard telephone line connectors, except that they have a set of eight wires instead of four, which makes the clip wider and thicker than a telephone connector. The socket into which the RJ-45 fits can be found on practically all Ethernet devices, including Crestron control systems, TPS touchpanels and CEN devices.



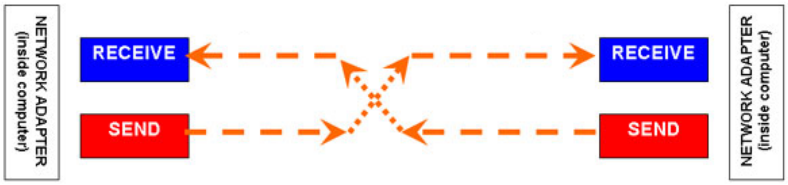
The most popular type of Ethernet cabling, and the type that Crestron recommends for use in e-Control, is **twisted-pair**, which looks like an ordinary telephone cable, except that it has eight wires inside instead of four.

Twisted-pair cabling is available in different grades or **categories**. About 85% of the networks in the U.S. use standard **unshielded twisted-pair (UTP) Category 5** cable because it offers a performance advantage over lower grades, and because it supports both Ethernet and Fast Ethernet networks. Crestron recommends using UTP Cat 5 cabling for use in e-Control.

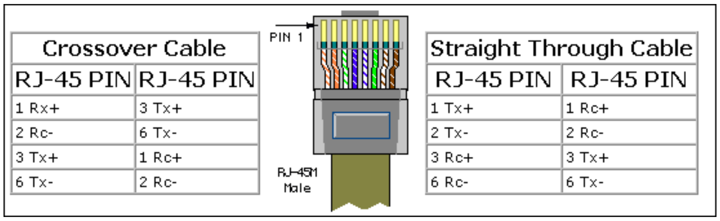
The most common type of network cable is a **straight-through** cable, which, as its name indicates, allows data to travel along a straight path through the cable to its destination. A straight-through cable is used to connect a computer, control system, or touchpanel to a hub or switch. This is because the **send** and **receive** connections on the hub or switch are the reverse of those on the device's network card or adapter. Thus, data goes "straight" from a send connection on the device to a receive connection on the hub or switch.



In contrast, crossover cables are useful for connecting any two network devices whose send and receive connections are the same. For example, many cable modems require a crossover cable to connect to a router. Here the cable "crosses" connections, allowing send connections to be directed to receive connections, and vice versa.



You should always know the type of cable a connection requires.



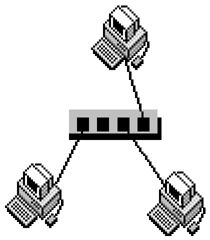
| Crossover Cable | |
|---|---|
| RJ-45 PIN | RJ-45 PIN |
| 1 Rx+ | 3 Tx+ |
| 2 Rc- | 6 Tx- |
| 3 Tx+ | 1 Rc+ |
| 6 Tx- | 2 Rc- |

PIN 1
RJ-45M
Male

| Straight Through Cable | |
|---|---|
| RJ-45 PIN | RJ-45 PIN |
| 1 Tx+ | 1 Rc+ |
| 2 Tx- | 2 Rc- |
| 3 Rc+ | 3 Tx+ |
| 6 Rc- | 6 Tx- |

When UTP Cat 5 cabling is used, straight-through cabling is inserted between each network device and the hub or switch. If you have five devices, you'll need five cables.

Each cable cannot exceed 328 feet in length. When viewed from above, a 10BaseT network forms a star configuration. That is, the cables from all of the devices converge at a common point. As shown in the figure, three computers are connected with 10BaseT cabling and a hub.



A 10BaseT hub is simply a box with a row of 10BaseT jacks. Most hubs have five, eight, 12, or 16 jacks, but some may have more. Most hubs also have an **uplink port**, which is a special port that allows the hub to be connected to other hubs. Uplink ports are the reverse of the other regular ports on the hub or switch. This is useful for "daisy-chaining" network connection devices so you can add ports.

To connect two 5-port switches together, for instance, you could connect one end of a straight-through cable to the uplink port on the back of the first switch, and connect the other end of the cable to any available *regular* port on the second switch. This would effectively add four more ports to the network.

A hub differs from a switch in that hubs use **shared bandwidth**, meaning that they must share their speed across the total number of ports on the device. As an example, a 10Mbps 5-port hub shares its 10Mbps speed across the five ports. Thus, if five devices are connected to five ports, each port can only transfer data at a rate of 2Mbps, because 10 divided by 5 equals 2. A 100Mbps 10-port hub with 10 devices connected to it shares the 100Mbps across the 10 ports, for a speed of 10Mbps per port. In addition, the duplex type of the device contributes to the total throughput of the device.

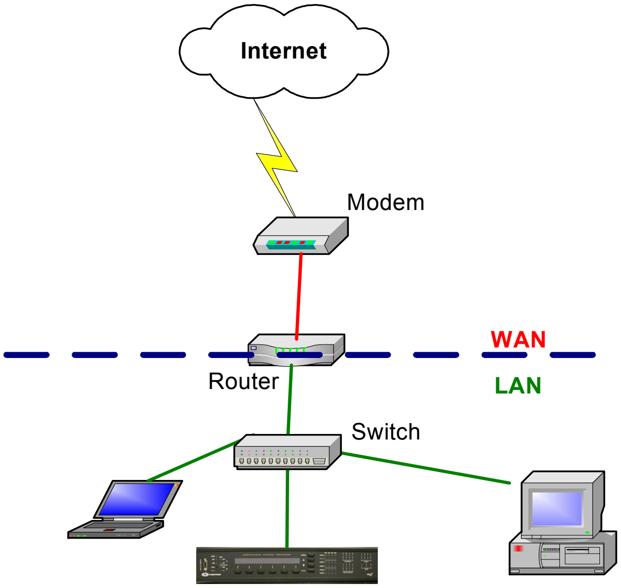
Switches, on the other hand, use **dedicated bandwidth**. Each port on a switch is given the full speed of the switch. Therefore, a 100Mbps 5-port switch with five devices attached would transfer data at 100Mbps over every port — an obvious advantage over a hub. Switches are usually more expensive than hubs, but the performance is better. Duplex is a factor in total performance as well.

***10/100 Ethernet Cabling Distances***

| Connection | Speed | Maximum Distance |
|---|---|---|
| Hub to Hub (without a switch) | 10Mbps | 100 meters/328 feet |
| Hub to Hub (without a switch) | 100Mbps | 10 meters/32.8 feet |
| Hub to Switch | 100Mbps | 100 meters/328 feet |
| PC to Hub/Switch | 100Mbps | 100 meters/328 feet |
| Crestron Control System to Hub/Switch (2-Series and X-Series) | 10Mbps | 100 meters/328 feet |
| Crestron Control System to Hub/Switch (2-Series only) | 100Mbps | 100 meters/328 feet |
| Crestron touchpanel to Hub/Switch (TPS-ENET only) | 10Mbps | 100 meters/328 feet |
| Crestron touchpanel to Hub/Switch (TPS-ENET only) | 100Mbps | 100 meters/328 feet |
| Crestron CEN device to Hub/Switch | 10Mbps | 100 meters/328 feet |

## Internet Routers

Internet security is an important consideration in networking, since any networked device with access to the Internet is, to some degree, at risk for unauthorized access. Fortunately, protecting a network is both inexpensive and easy. The most simple and flexible way to build an Internet **firewall** (network shield from unauthorized access) is to install a piece of hardware into the network that already has firewall software built into it. The most commonly used firewall device is an Internet **router**.



An Internet router is installed between an Internet connection and the rest of the network. It protects the network by making individual computers, control systems, and other Ethernet devices "invisible" to the outside world. The only externally recognized device is the router itself. Put another way, a router is a network device with two sides: one side is made up of the private LAN of PCs, control systems, touchpanels, etc. which this reference guide sometimes calls the "internal LAN." The other, public side is the Internet, or the WAN. We will see that in some applications the "public" side can also be a corporate or residential LAN, with the "internal" side being a sub-network within that LAN.

The router's firewall (NAT, or **N**etwork **A**ddress **T**ranslator) protects the internal LAN by inspecting the data coming in from the WAN port before delivery to the final destination on the LAN port. The router inspects Internet port services like the Web server, FTP server, or other Internet applications, and, if allowed, it will forward the data to the appropriate PC or control system on the LAN side.

In this way, an Internet router accomplishes two separate but related tasks. First, it protects the network from unwanted access and/or unneeded information. Second, it routes information to the intended destination.

## Crestron NAT

Crestron manufactures an Ethernet network card for its 2-Series control systems called the C2ENET-2 card, which provides two RJ-45 Ethernet ports (labeled LAN A and LAN B). The card works with an internal NAT on the 2-Series processor that enables programmers to create a sub-network within a larger corporate or residential LAN. Here the card's LAN A port is the public side that is visible to the larger network, while the LAN B port connects to the private, internal LAN of e-Control devices.

# IP Communication

The Ethernet standard supports numerous communication protocols that determine how data is transferred from one network node to another. Different protocols work together at different levels, or **layers**, as outlined by the **OSI reference model**, to enable communication on a network. The OSI reference model separates node-to-node communications into seven layers, each building upon the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the application-program level. (The OSI model is explained more in detail in “Appendix B: The OSI Reference Model” on page 55.)

**TCP/IP** is the suite (or stack) of networking protocols that make up the Internet and most LANs. The TCP/IP name is taken from two of the core protocols in the suite, IP (**I**nternet **P**rotocol) and TCP (**T**ransport **C**ontrol **P**rotocol. Another core protocol in the suite is UDP (**U**ser **D**atagram **P**rotocol).

Crestron equipment communicates over Ethernet using a proprietary protocol called CIP (**C**restron over **I**nternet **P**rotocol), which is an implementation of UDP. Crestron also provides hardware and software gateways that convert data received over TCP into CIP, and vice-versa.

Both UDP and TCP are transport-layer (layer 3) protocols that run over IP networks. UDP has several characteristics that make it convenient and useful for e-Control. First, UDP is *connectionless*, meaning that Crestron equipment can transfer data over Ethernet without prior advertising or need to negotiate a connection. UDP has minimal overhead; each datagram on the network is composed of just a small header and the control data. In addition, UDP allows data to be broadcast to multiple devices. UDP thus provides simple, fast, and efficient transfer of data.

In contrast, TCP is a connection-oriented protocol. Before data transfer can take place, a connection must first be established; after data transfer, the connection must be torn down. TCP incurs much more overhead than UDP because it provides extensive error checking and flow control. This makes TCP a more reliable, yet slower transmission.

## IP Addressing

Both UDP and TCP use the same addressing scheme; that is, they use **IP addresses** to identify devices (hosts) connected via Ethernet to other hosts. Every host on an IP network must have a unique IP address to identify its “location,” or address, on the network. This applies to both the WAN and LAN connections.

The IP address is a 32-bit binary number that is expressed in “dotted quad” format, consisting of the decimal values of its four octets (bytes) separated by periods. For example, the IP address 192.168.123.132 is the decimal equivalent of the binary number 11000000.10101000.01111011.10000100.

The decimal numbers separated by periods are the octets converted from binary to decimal notation.

The first part of an IP address identifies the network; the last part identifies the host, or node. If you take the example 192.168.123.132 and divide it into these two parts you get 192.168.123.0 as the **network address**; and 0.0.0.132 as the **host address**.

### *Network Classes*

Internet addresses are allocated by the InterNIC, the organization that administers the Internet. These public IP addresses are divided into **classes**, the most common being A, B, and C. The class of a network depends on its size.

You can identify the class of an IP address by looking at its first octet, as follows:

- **Class A** addresses are for large networks with many devices. These networks have 0-127 as their first octet. The address 10.52.36.11 is a Class A address. Its first octet is 10, which is between 1 and 126, inclusive.

  Class A networks can have up to 16,777,214 hosts.

- **Class B** addresses are for medium-sized networks. These networks have 128-191 as their first octet. The address 145.16.52.63 is a Class B address. Its first octet is 145, which is between 128 and 191, inclusive.

  Class B networks can have up to 65,534 hosts.

- **Class C** addresses are for small networks. These networks have 192-223 as their first octet. The address 198.145.123.132 is a Class C address. Its first octet is 198, which is between 192 and 223, inclusive.

  Class C networks can have up to 254 hosts.

### *IP Subnet Masking*

Applying a **subnet mask** to an IP address allows an Internet router to identify the “network” and “node” parts of the address. The 1s in the mask represent the network bits, and the 0s in the mask represent the node bits. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the network address. For example:

```
10010110.11010111.00010001.00001001     150.215.017.009 (IP address)
11111111.11111111.00000000.00000000     255.255.000.000 (subnet mask)
-----------------------------------------------------------
10010110.11010111.00000000.00000000     150.215.000.000 (network address)
```

This result may seem familiar because Class A, B and C addresses have a self-encoded or default subnet mask built in:

```
Class A - 255.0.0.0              11111111.00000000.00000000.00000000
Class B - 255.255.0.0            11111111.11111111.00000000.00000000
Class C - 255.255.255.0          11111111.11111111.11111111.00000000
```

### *Private Subnets*

Three specific ranges of IP network addresses have been set aside for internal use, meaning that they are not routable on the Internet. These addresses are considered **unregistered**. No company or agency can claim ownership of unregistered addresses or use them on public computers. Routers are designed to discard (instead of forward) unregistered addresses.

The private network addresses are as follows:

- **Range 1: Class A** - 10.0.0.0 through 10.255.255.255
- **Range 2: Class B** - 172.16.0.0 through 172.31.255.255
- **Range 3: Class C** - 192.168.0.0 through 192.168.255.255

You are not required to use any particular range when you set up an internal network. However, Crestron recommends using the private network addresses for e-Control equipment on an internal LAN, because they greatly reduce the chance of an IP address conflict.

Another reserved IP address is 127.0.0.1, or **localhost**. This special address is also referred to as a **loopback** address and represents the same computer or device on which a TCP/IP message originates. Data going to 127.0.0.1 does not actually go out to the Internet.

### *Default Gateway*

A **default gateway** is a router that links a subnet, or internal LAN, to outside networks. When a device attempts to communicate with another device on the same internal LAN, the data is simply transferred on the local subnet. However, if the destination is a remote device, then the data has to be forwarded to the default gateway. It is then the responsibility of the router to forward the data to the correct subnet.

In cases where data will not be routed outside the internal LAN, the default gateway address can be set to 0.0.0.0. Otherwise, you would specify the internal LAN address of the router.

### *Static and Dynamic IP Addressing*

Static and dynamic IP addressing are two different methods of assigning an IP address to a device.

A static IP address is a fixed IP address that you assign manually to a computer or network device. It remains valid until it is disabled; static IP addressing thus ensures that a device will always have the same IP address until it is changed to a different value.

Crestron's X-Series control systems and CEN devices require static IP addressing for use in e-Control.

In contrast, a dynamic IP address is automatically assigned to a device on the network. These IP addresses are called "dynamic" because they are only temporarily assigned, or leased, to the device. After a certain time they expire and may change. When a device connects to the network (or the Internet) and its dynamic IP address has expired, the DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) server will assign it a new dynamic IP address.

The purpose of DHCP is to let network administrators centrally manage and automate the assignment of IP addresses in an organization's network. DHCP greatly reduces the work necessary to administer a large IP network. Without DHCP, the administrator has to manually configure the IP address each time a computer is added to the network or moves to a different location.

DHCP provides integration with a DNS (**D**omain **N**ame **S**ystem) service. This system allows hosts to have both domain name addresses (such as ftp.crestron.com) and IP addresses (such as 65.206.113.4). The domain name address is easier for people to remember and is automatically translated into the numerical IP address.

The domain name address (also called the **F**ully-**Q**ualified **D**omain **N**ame, or FQDN) identifies the owner of that address in a hierarchical format: *server.organization.type.* For example, ftp.crestron.com identifies the FTP server at Crestron, with ".com" signifying a commercial organization.

A DNS server, also called a **name server**, maintains a database containing the host computers and their corresponding IP addresses. Presented with the domain name address ftp.crestron.com, for example, the DNS server would return the IP address 65.206.113.4.

Another name-resolution service is WINS (**W**indows **I**nternet **N**aming **S**ervice). WINS is used in conjunction with DNS and DHCP in a Windows NT 4.0 Server environment.

Crestron's 2-Series control systems and TPS touchpanels support DHCP in a Windows 2000 Server or Windows NT 4.0 Server environment.

### Obtaining IP Information

If you are setting up a residential LAN, you must obtain the IP address and other IP configuration information for the WAN side of the router from the ISP. You would then use the router's network configuration screens to define the range of static IP addresses available on the LAN side.

If you are installing e-Control in a corporate LAN, the network administrator must provide you with static IP addresses if you are configuring X-Series and CEN equipment. In addition to the static IP address of each device, the network administrator will give you the subnet mask and default gateway address of the network.

For 2-Series control systems and TPS touchpanels, you can configure the equipment to accept dynamic IP addresses from the Windows DHCP Server.

If you are using the NAT on the C2ENET-2 card, you can configure the LAN A side for static or dynamic IP addressing. Then you can assign static IP addresses for devices on the LAN B side, using the range of private IP addresses.

## Port Numbers

Any server machine makes its services available to the Internet using numbered **ports**, one for each service. For example, if a server machine is running a Web server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. Clients connect to a service at a specific IP address *and* on a specific port number. There are 65,535 port numbers available for use with TCP, and the same number is available for UDP.

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

- The Well Known Ports are those from 0 through 1023.

- The Registered Ports are those from 1024 through 49151—Crestron has four registered ports for CIP and TCP communication.
- The Dynamic and/or Private Ports are those from 49152 through 65535.

Some examples of well-known port numbers are FTP (port 21), Telnet (port 23), E-mail (SMTP, or Simple Mail Transfer Protocol, port 25) and WWW (port 80).

If the server machine accepts connections on a port from the outside world, and if a firewall is not protecting the port, you can connect to the port from anywhere on the Internet and use the service.

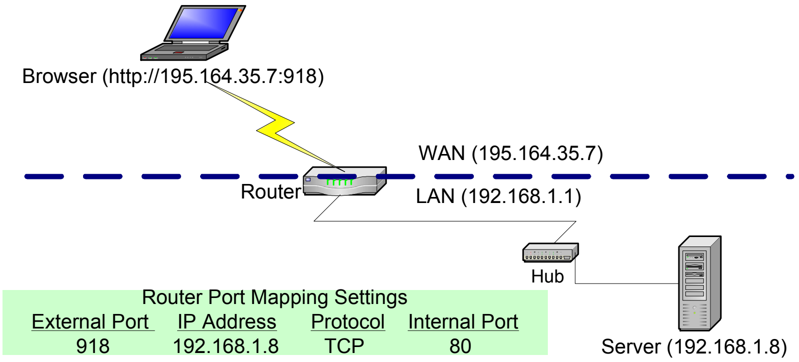
Note that nothing forces a Web server, for example, to be on port 80. If you were to set up your own Web server, you could put it on port 49153 or any other unused port. Then if the server were located at **http://www.e-control.com**, someone on the Internet could connect to that server by typing http://www.e-control.com:49153. The ":49153" explicitly specifies the port number, and would have to be included for someone to reach the server. When no port is specified, the browser simply assumes that the server is using the well-known port 80.

## Port Mapping

If a firewall or NAT is protecting a port, an Internet client can still access a server machine on the internal LAN if the router or NAT is configured for **port mapping**. Port mapping is a mechanism that makes specific services available to the WAN without exposing other areas of the internal LAN.

Here you assign an "external" port number to whichever service you want to make available to the outside world; the external port is mapped to the real port number on the internal LAN. This allows anyone on the outside to connect to the server, if they know the IP address or domain name address of the router and the external port number of the server.

For example, if you were to set up a Web server on the internal LAN, you could assign it an external port number 918, and map it to internal port 80. Any Internet client that wants to connect to that server would then need to know the IP address of the router, and the external port number. If the router were located at IP address 195.164.35.7, the client would enter http://195.164.35.7:918, as shown below.



Router Port Mapping Settings

| External Port | IP Address | Protocol | Internal Port |
|---|---|---|---|
| 918 | 192.168.1.8 | TCP | 80 |

Most routers allow between 10 and 16 ports to be opened using port mapping; the Crestron NAT that is built into the 2-Series processor allows up to 16.

## Secure Sockets Layer

Crestron 2-Series control systems are the first in the AV industry to provide built-in support for SSL, **S**ecure **S**ockets **L**ayer, the de facto standard for protecting Web-based communication between clients and servers. SSL is a protocol that provides a secure channel for communication between two machines. The secure channel is transparent, which means that it passes the data through, unchanged. The data is encrypted between the client and the server, but the data that one end writes is exactly what the other end reads. The SSL protocol uses TCP as the medium of transport.

SSL ensures that the connection between a Web browser and Web server is secure by providing **authentication** and **encryption**. Authentication confirms that servers, and sometimes clients, are who they say they are. Encryption creates a secure “tunnel” between the two, which prevents unauthorized access to the system.

The secure tunnel that SSL creates is an encrypted connection that ensures that all information sent between the client and server remains private. SSL also provides a mechanism for detecting if someone has altered the data in transit. If at any point SSL detects that a connection is not secure, it will terminate the connection and the client and server will have to establish a new, secure connection.

SSL uses both **public-key** and **symmetric key** encryption techniques. Public keys are a component of public-key cryptographic systems. The sender of a message uses a public key to encrypt data; the recipient of the message can only decrypt the data with the corresponding private key. Public keys are known to everybody, while private keys are secret and only known to the recipient of the message. Since only the server has access to its private key, only the server can decrypt the information. This is how the information remains confidential and tamper-proof while in transit across the network.

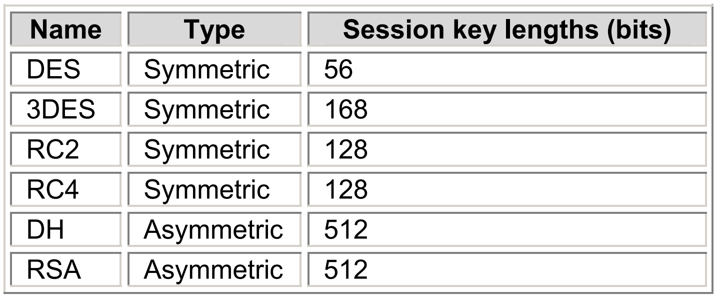
An SSL transaction consists of two distinct parts: the key exchange, and the bulk data transfer. The SSL Handshake Protocol handles key exchange and the SSL Record Protocol handles the bulk data transfer.

The key exchange (SSL handshake protocol) begins with an exchange of messages called the SSL handshake. During the handshake, the server authenticates itself to the client using public-key encryption techniques. Then the client and the server create a set of symmetric keys that they use during that session to encrypt and decrypt data and to detect if someone has tampered with the data. Symmetric key encryption is much faster than public-key encryption, while public-key encryption provides strong authentication techniques.

Once the key exchange is complete, the client and the server use this session key to encrypt all communication between them. They do this encryption with a **cipher**, or symmetric key encryption algorithm, such as RC4 or DES. This is the function of the SSL Record Protocol. There are two types of ciphers, symmetric and asymmetric. Symmetric ciphers require the same key for encryption and decryption, whereas with asymmetric ciphers, data can be encrypted using a public key, but decrypted using a private key.

SSL supports a variety of ciphers that it uses for authentication, transmission of certificates, and establishing session keys. SSL-enabled devices can be configured to support different sets of ciphers, called **cipher suites**.

Crestron's implementation of SSL is based on OpenSSL (www.openssl.org), version 0.9.6a. The encryption algorithms and the key lengths supported in the 2-Series processor are as follows:



| Name | Type | Session key lengths (bits) |
|---|---|---|
| DES | Symmetric | 56 |
| 3DES | Symmetric | 168 |
| RC2 | Symmetric | 128 |
| RC4 | Symmetric | 128 |
| DH | Asymmetric | 512 |
| RSA | Asymmetric | 512 |

SSL-enabled clients and servers confirm each other's identities using **digital certificates**. Digital certificates are issued by trusted third-party enterprises called Certificate Authorities, or CAs. From the certificate, the sender can verify the recipient's claimed identity and recover their public key. By validating digital certificates, both parties can ensure that an imposter has not intercepted a transmission and provided a false public key for which they have the correct private key.

A CA-signed certificate provides several important capabilities for a Web server:

- Browsers will automatically recognize the certificate and allow a secure connection to be made, without prompting the user. (If a browser encounters a certificate whose authorizing CA is not in its list of trusted CAs, the browser will prompt the user to accept or decline the connection.)
- When a CA issues a signed certificate, they are guaranteeing the identity of the organization that is providing the Web pages to the browser.

Alternatively, **self-signed certificates** can be generated for secure Web servers, but self-signed certificates do not provide the same functionality as CA-signed certificates. Browsers will not automatically recognize a self-signed certificate; and a self-signed certificate does not provide any guarantee concerning the identity of the organization that is providing the server.

In addition, handshaking is much faster in the case of CA-signed certificates because the process of creating private/public keys is CPU intensive. With self-signed certificates, these keys are created at every instance of a handshake, whereas with CA-signed certificates the keys are already loaded. A CA-signed certificate thus provides many important capabilities for a secure server.

There are various Certificate Authorities, notable among them being Thawte and Verisign. For a fee, a CA investigates the organization hosting the server and issues a certificate vouching for the identity of the server. The procedure for obtaining/enrolling for a CA-signed certificate varies with each CA and is described on their Web sites. However, all CAs require a CSR, or **C**ertificate **S**igning **R**equest. The CSR can be copied and pasted to the online enrollment form or sent via e-mail to the CA, along with any other pertinent information the CA requires. The CA then issues the certificate, usually via e-mail. The Crestron Viewport provides all the certificate management tools necessary to generate a CSR and upload the certificate to the 2-series processor.

The CA-signed certificate is an ASCII "base64" encoded text (*.CER) file, which the 2-Series processor converts to a binary file called \\SYS\srv_cert.der. As a part of the CSR process, a private key is also created as \\SYS\srv_key.der. It is extremely important to back up the private key, as it is unique to each CSR. If the private key is lost the certificate is useless and it would be necessary to begin the enrollment process all over again.

Here is a description of an SSL transaction:

1. The browser sends a request for an SSL session to the Web server.
2. The Web server sends the browser its digital certificate. The certificate contains information about the server, including the server's public key.
3. The browser verifies that the certificate is valid and that a trusted CA issued it.
4. The browser generates a "master secret" that is encrypted using the server's public key and sent to the Web server.
5. The Web server decrypts the master secret using the server's private key.
6. Now that both the browser and the Web server have the same master secret, they use this master secret to create keys for the encryption and MAC (message authentication code) algorithms used in the bulk-data process of SSL. Since both participants used the same master key, they now have the same encryption and MAC keys.
7. The browser and Web server use the SSL encryption and authentication algorithms to create an encrypted tunnel. Through this encrypted tunnel, they can pass data securely through the network.

Though the authentication and encryption process may seem involved, the user generally does not even know it is taking place. However, the user will be able to tell when the secure tunnel has been established since most SSL-enabled Web browsers will display a small closed lock at the bottom (or top) of their screen when the connection is secure. Users can also identify secure Web sites by looking at the Web site address; a secure Web site's address will begin with http**s**:// rather than the usual http://. The Web server listens for a secure connection on the well-known port 443.

# e-Control Hardware Configuration

This section describes how to configure X-Series and 2-Series equipment for integration into a LAN.

## Windows DHCP/DNS Server Configuration

Crestron's 2-Series control systems (minimum CUZ 3.041) and TPS touchpanels support DHCP in the following environments:

- Windows 2000 Server with DHCP Server and DNS Server (Dynamic DNS enabled)
- Windows NT 4.0 Server with DHCP Server and WINS Server

In the configuration requirements below, a *scope* defines the range of IP addresses for the network. Typically a scope defines a single physical subnet on the network. Scopes provide the primary way for the DHCP server to manage distribution and assignment of IP addresses and any related configuration parameters to clients on the network.

*Scope options* are client configuration parameters applied specifically to all clients that obtain a lease within a particular scope. Some commonly used options include IP addresses for default gateways (routers), WINS servers, and DNS servers.

The network administrator should configure the Windows Server as follows:

**Configuration 1: DHCP + Dynamic DNS (Windows 2000 only)**

The network administrator should configure the DHCP scope to include the following scope options:

- 003 - Router
- 006 - DNS Servers
- 015 - Domain Name

The DHCP scope should also have the following options enabled:

- Always dynamically update all nodes
- Enable updating of nodes that don't support dynamic DNS

The DNS Server should have the following option enabled:

- Enable WINS Resolution (Windows (NT 4.0)
- Enable WINS Forward Lookup (Windows 2000)

**Configuration 2: DHCP + DNS + WINS (Windows NT 4.0 and Windows 2000)**

The network administrator should configure the DHCP scope to include the following scope options:

- 003 - Router
- 006 - DNS Servers
- 015 - Domain Name

- 044 - WINS/NBNS Servers
- 046 - WINS/NBT Node Type (set value to “0x2”)

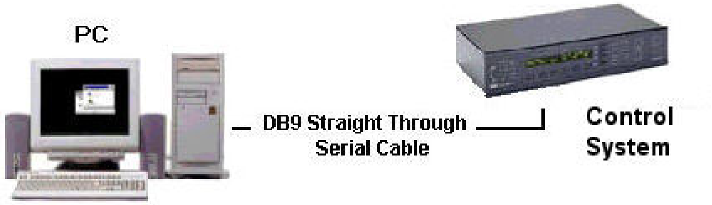
The DNS Server should have the following option enabled:

- Handle Dynamic Updates (Windows 2000 only)

## Control Systems

Before setting the control system’s IP information for the first time, use the Crestron Viewport to establish a serial connection to the unit, as follows:

1. Use a DB9 straight-through serial cable to connect a COM port on the PC to the COMPUTER port on the control system.

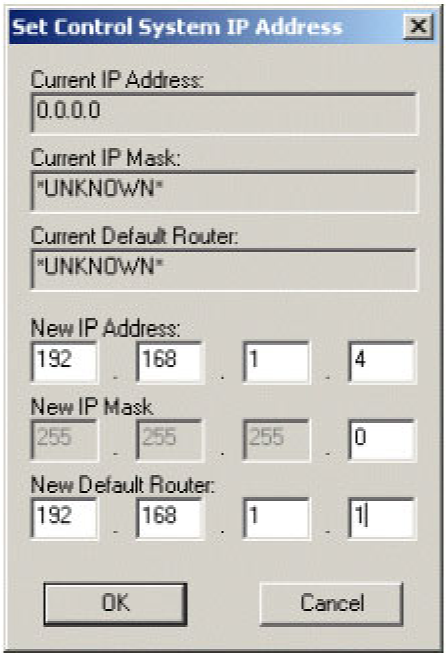


2. Start the Crestron Viewport and click **Communication Settings** on the **Setup** menu. Select **RS-232** as the connection type. Then set the PC to match the communication settings of the control system:
    - Port = COM 1. Select the PC COM port (COM 1 - COM 8).
    - Baud rate = 115200 for 2-Series processors; 57600 for X-Series.
    - Parity = None.
    - Number of data bits = 8.
    - Number of stop bits = 1.
    - Hardware handshaking (RTS/CTS) enabled.
    - Software handshaking (XON/XOFF) not enabled.

When communication is established, the title bar at the top of the Viewport screen will display the serial settings, i.e., “COM1 115200 N81 RTS/CTS”. You can also click **Establish Communication** on the **Diagnostics** menu to verify communication.

### *X-Series Control Systems*

1. **CNXENET and CNXENET+** cards: Click **Set Control System IP Information** on the **Functions** menu.
2. Enter the static IP address of the control system. In the following example, the control system is assigned the private IP address 192.168.1.4. The example also shows the default subnet mask for that address class (Class C), 255.255.255.0.



Set Control System IP Address

Current IP Address: 0.0.0.0

Current IP Mask: *UNKNOWN*

Current Default Router: *UNKNOWN*

New IP Address: 192 . 168 . 1 . 4

New IP Mask: 255 . 255 . 255 . 0

New Default Router: 192 . 168 . 1 . 1

3. Enter the default router address. In residential applications, this is the internal LAN address of the router, not the WAN IP address that is visible to the outside. In the example above, the default router address is 192.168.1.1, which is the default address used by router manufacturers such as Linksys. If data will not be routed to outside subnets, you can set the default router address to 0.0.0.0.
4. When you are satisfied with the IP settings click **OK** to reboot the control system.

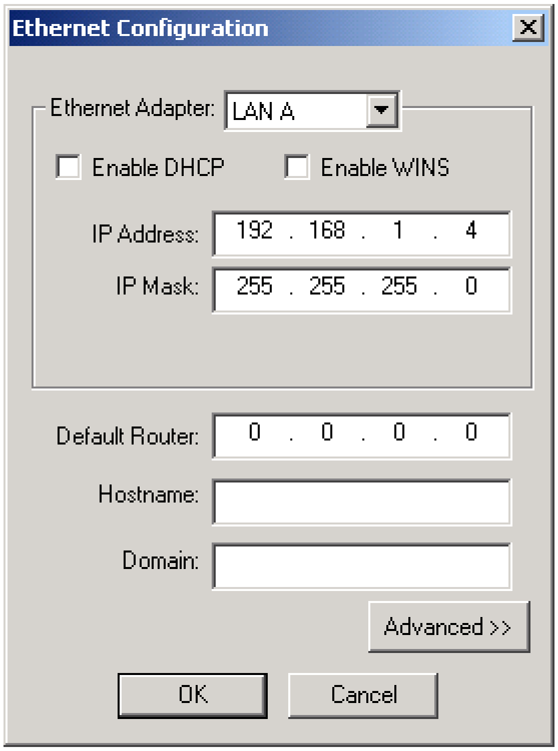
### *2-Series Control Systems*

**C2ENET-1 and C2ENET-2** cards: The C2ENET cards provide two configuration options: one for LAN A and the other for LAN B. With the C2ENET-1 card, values should only be entered for LAN A.

**For static IP addressing**, enter the IP information just as described for the CNX-ENET and CNX-ENET+ cards.

1. Enter the static IP address of the control system.
2. Enter the subnet mask.
3. Enter the default router address (if data will not be routed to outside subnets, this value can be set to 0.0.0.0).

   In the following example, the control system will be set to the IP address 192.168.1.4. The subnet mask is the default for that address class (Class C), 255.255.255.0, and the default router address will be set to 0.0.0.0.



Ethernet Adapter: LAN A

□ Enable DHCP □ Enable WINS

IP Address: 192 . 168 . 1 . 4

IP Mask: 255 . 255 . 255 . 0

Default Router: 0 . 0 . 0 . 0

Hostname:

Domain:

4. Static IP values can be set for the LAN B side of the C2ENET-2 card the same way. Simply select **LAN B** from the **Ethernet Adapter** list.

   As described previously, the C2ENET-2 card allows you to create a sub-network within a larger corporate or residential LAN. Here LAN A is the public side that is visible to users on the larger network, while LAN B is the internal LAN of e-Control devices. In this way, a network administrator would need to provide one static IP address, for the public (LAN A) side. Alternatively, the LAN A side can be configured for dynamic IP addressing.

   When assigning an IP address for LAN B, it is recommended that you choose from the private IP address classes described earlier.

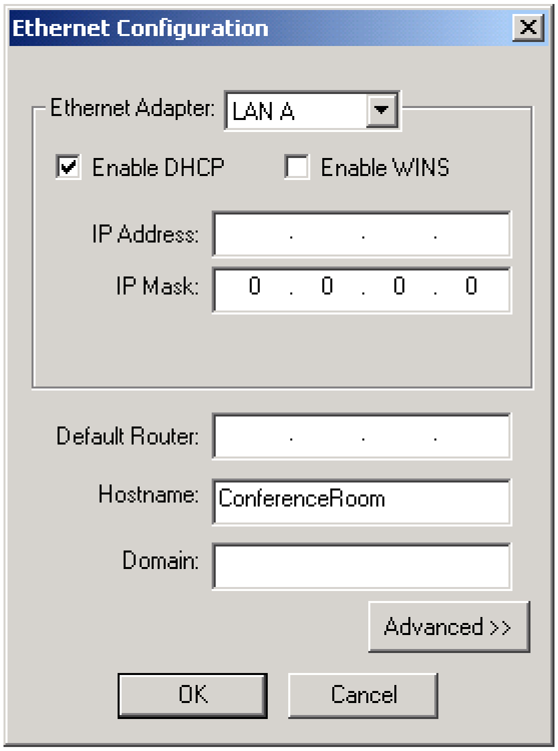
   The network addresses of LAN A and LAN B cannot be the same. For example, if the same subnet mask is applied to both IP addresses and the resulting network address is 192.168.1.0, then an error message will be generated.

**For dynamic IP addressing:**

1. Select the **DHCP** check box to enable DHCP with Windows 2000 Server; for Windows NT 4.0 Server, select *both* the **DHCP** and the **WINS** check boxes. (The IP address and IP mask fields will be ignored if either check box is selected.)
2. Enter the hostname of the control system in the **Hostname** field. The hostname identifies the machine on the network and is automatically translated into the numerical IP address. The hostname can consist of up to 64 characters. Valid characters are 0 – 9, A – Z (not case-sensitive), and the

dash (hyphen character). No other characters are valid. The hostname cannot begin with a dash or number.

3. The IP address of the default router is provided by the DHCP server and thus the **Default Router** field should be left blank.



Ethernet Adapter: LAN A

☑ Enable DHCP □ Enable WINS

IP Address: . . .

IP Mask: 0 . 0 . 0 . 0

Default Router: . . .

Hostname: ConferenceRoom

Domain:

4. If applicable, enter the domain in the **Domain** field. This is only necessary if you are configuring DHCP on an Ethernet connection to a control system that currently has a static address. The domain name will be used to reconnect to the control system after it reboots. With a serial connection, the domain does not need to be entered.

   Note that the domain supplied by the DHCP server will overwrite the domain that is indicated in this field.

**Advanced Settings** (optional):

1. Click the **Advanced** button to set optional parameters. You can enter the IP address of the primary DNS server in the **DNS Server 1** field; enter the IP address of the secondary DNS Server in field 2.

   If the DHCP server provides the address for the DNS server, it is not necessary to enter these values. Here the DNS server addresses will automatically be filled in.

2. You have the option to change the CIP and CTP port numbers in rare cases where a network conflict may exist with ports 41794 and 41795.

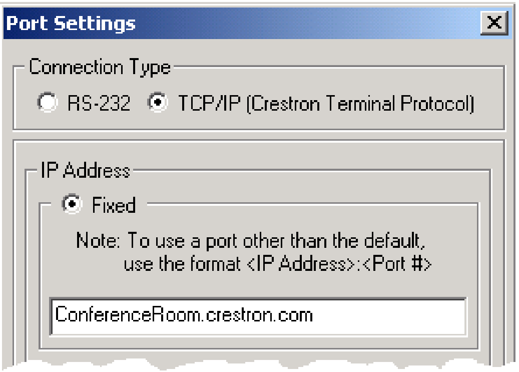
   The Web port can be changed for security reasons if no firewall or router is protecting the network. To prevent attacks by hackers the port can be moved to another value. Users on the LAN would then have to specify the port number in the URL, i.e., http//www.crestron.com:49153 where the value after the colon indicates the Web port.

In most cases, the port numbers do not need to be changed.

3. The **Enable Web Server** check box turns the Web server on and off.
4. When you are satisfied with the IP settings click **OK** to reboot the control system.

Once you have set the IP information for the control system, it becomes possible to communicate with the console via TCP/IP.

Click **Communication Settings** on the Viewport **Setup** menu and choose **TCP/IP** as the connection type. Then enter the IP address or fully qualified domain name of the control system.



Port Settings

Connection Type

○ RS-232 ● TCP/IP (Crestron Terminal Protocol)

IP Address

● Fixed

Note: To use a port other than the default, use the format <IP Address>:<Port #>

ConferenceRoom.crestron.com

Here the Viewport title bar will display the new communication settings, i.e., "Connected to ConferenceRoom.crestron.com on Port 41795".

### *2-Series SSL Configuration*

This section describes the steps involved in enabling the 2-Series Web server for SSL and obtaining a digital certificate from a Certificate Authority. The steps are summarized as follows (each step is described in detail later):

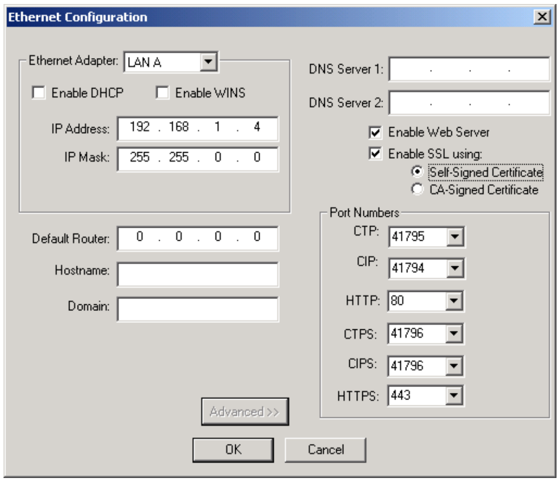
- Establish a serial connection to the 2-Series control system.
- Enable SSL using a self-signed certificate.
- Create an encryption public/private key pair and a certificate-signing request (CSR) based on the public key.
- Back up the private key.
- Send the CSR to a Certificate Authority such as Thawte or Verisign, who will verify the identity of the requestor and issue a signed certificate.
- Install the CA-signed certificate and optionally, the root certificate, to the 2-Series processor.
- Enable SSL using the CA-signed certificate.

### 2-Series Control System Requirements

- CUZ: 3.055 or later
- Viewport: 3.53 or later
- SIMPL Windows: 2.04.11

### Enable SSL with a self-signed certificate

1. Establish a serial connection to the 2-Series control system.
2. On the Viewport **Functions** menu, click **Set Control System IP Information**.
3. Click the **Advanced** button, and then click **Enable SSL**.
4. Select **Self-Signed Certificate** and click **OK** to reboot the control system.



Ethernet Configuration

Ethernet Adapter: LAN A

□ Enable DHCP □ Enable WINS

IP Address: 192 . 168 . 1 . 4

IP Mask: 255 . 255 . 0 . 0

Default Router: 0 . 0 . 0 . 0

Hostname:

Domain:

DNS Server 1: . . .

DNS Server 2: . . .

☑ Enable Web Server

☑ Enable SSL using:

● Self-Signed Certificate

○ CA-Signed Certificate

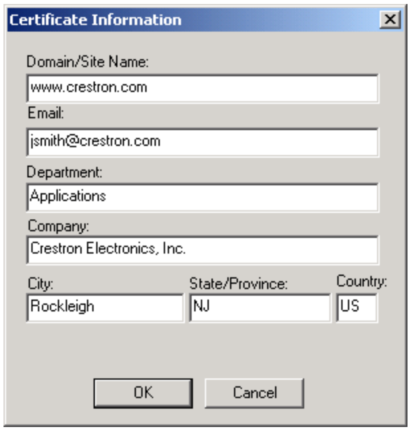
Port Numbers

| | |
|---|---|
| CTP: | 41795 |
| CIP: | 41794 |
| HTTP: | 80 |
| CTPS: | 41796 |
| CIPS: | 41796 |
| HTTPS: | 443 |

5. This generates a self-signed certificate that you can use temporarily while you obtain a CA-signed certificate. Alternatively, you can continue to use the self-signed certificate so long as the client is interested only in data encryption and not server identity.

### Generate a Certificate Signing Request (CSR)

1. On the Viewport **File Transfer** menu, point to **Generate Certificate Request**, and then click **Generate Certificate**.



Certificate Information

Domain/Site Name: www.crestron.com

Email: jsmith@crestron.com

Department: Applications

Company: Crestron Electronics, Inc.

City: Rockleigh

State/Province: NJ

Country: US

2. Enter the information of the organization requesting the certificate. As shown in the previous diagram, the information includes the domain name of the organization, the e-mail address and department of the contact person making the request, the company name, city and state, and the two-letter country code. The two-character country codes correspond to ISO 3166 (International Standards Organization), and the complete list is available on their Web site: http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html

   The domain name is not transferable, and thus must be the one that will actually be used by clients. The domain name must be officially registered to the company; otherwise the certificate request will be rejected.

3. When you click **OK**, Viewport will generate the CSR and private key and automatically save the two files in the \SYS directory of the 2-Series processor. In addition, Viewport will prompt you to save the CSR file to a directory on your hard drive: Locate the target directory and click **Save**.

As described earlier, the CSR file is an ASCII text file that is saved in the \SYS directory as: **\\sys\request.csr**. The private key is also saved in the \SYS directory with a .der extension as: **\\sys\srv_key.der**. The procedure for backing up the private key is described in the next section.

The .csr text file is in the following format:

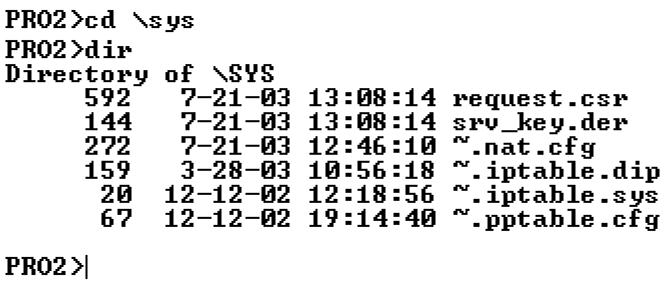
```
          -----BEGIN NEW CERTIFICATE REQUEST----
MIIBZzCCARECAQAwgZQxCzAJBgNVBAYTAlVTMRIwEAYDVQQIEwlob3N0c3RhdGUxETAPB
gNVBAcTCGhvc3RjaXR5MRUwEwYDVQQKEwxob3N0bmFtZSBpbmMxCjAIBgEAEwNNSVMxG
TAXBgNVBAMTEHd3dy5ob3N0bmFtZS5jb20xIDAeBgkqhkiG9w0BCQEWEWhvc3RAaG9zdG5hb
WUuY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMxVTzjNPVWjOHUtMzEsOEWRMIQ
WvilIYliVNtK7jTbyB8WUmucwz3JGfP1LZ5AvT5OQsz8tDsILYItGGliC2tcCAwEAAaAXMBUGCSq
GSIb3DQEJBzEIEwZleHRyYTEwDQYJKoZIhvcNAQEEBQADQQDLIuRV1NBOrlLr3XWI5XiHRH
CfQ8gpDOP5MDCdVFgDPvxi5TpQSFV/3PPUAm6BKAiZxmdpX8BUaEsRdQqNfof3
          -----END NEW CERTIFICATE REQUEST-----
```

When sending the CSR to a Certificate Authority it may be necessary to cut and paste the text between the “Begin new certificate request” and “End new certificate request” delimiters. To do this you can open the CSR file in a text editor such as Notepad.

### Backup the private key

1. Before backing up the private key, the processor’s \SYS directory should be the active directory so that Viewport can locate the file:

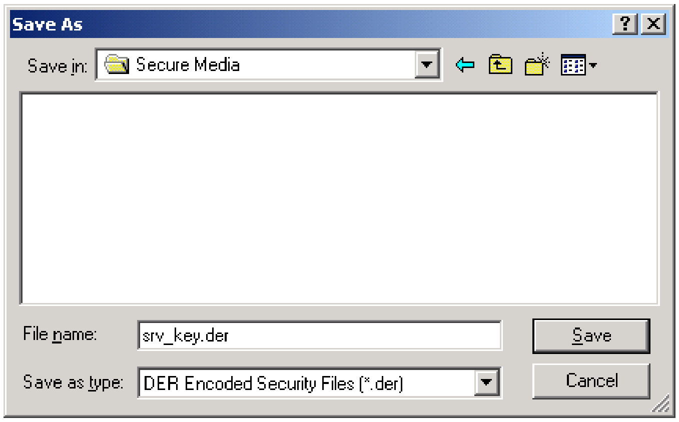
   On the Viewport command line, go to the \SYS directory by typing “cd \sys”. To open the directory type “dir”. This will display a list of files in the \SYS directory, including the CSR (**request.csr**) and the private key (**srv_key.der**).



```
PRO2>cd \sys
PRO2>dir
Directory of \SYS
     592   7-21-03 13:08:14 request.csr
     144   7-21-03 13:08:14 srv_key.der
     272   7-21-03 12:46:10 ~.nat.cfg
     159   3-28-03 10:56:18 ~.iptable.dip
      20  12-12-02 12:18:56 ~.iptable.sys
      67  12-12-02 19:14:40 ~.pptable.cfg

PRO2>
```

2. Now that \SYS is the active directory, click the Viewport **File Transfer** menu, point to **Generate Certificate Request**, and then click **Backup Key**. Viewport will automatically locate the **srv_key.der** file.



Save in: Secure Media

File name: srv_key.der

Save as type: DER Encoded Security Files (*.der)

3. Browse to the location where you want to store the .der file and click **Save**. Since the private key is unique to each CSR, it's a good idea to back up the file to secure media.

### Obtaining the Certificate

As described earlier, the exact procedure for obtaining a certificate differs depending on the CA, but in all cases you have to submit the CSR along with all verifying information that the CA requires. Here it may be necessary to open the CSR file in a text editor such as Notepad and copy and paste the text between the "Begin new certificate request" and "End new certificate request" delimiters before sending the file to the CA.

The time it takes to receive the certificate will vary based on how quickly the CA receives the required documentation.

### Upload the CA-Signed Certificate

Once the CA validates the CSR, the CA issues the certificate. The certificate is usually sent to the requester via e-mail, in the following format:

-----BEGIN CERTIFICATE-----
MIIBZzCCARECAQAwgZQxCzAJBgNVBAYTAlVTMRIwEAYDVQQIEwlob3N0c3RhdGUxETAPB
gNVBAcTCGhvc3RjaXR5MRUwEwYDVQQKEwxob3N0bmFtZSBpbmMxCjAIBgEAEwNNSVMxG
TAXBgNVBAMTEHd3dy5ob3N0bmFtZS5jb20xIDAeBgkqhkiG9w0BCQEWEWhvc3RAaG9zdG5hb
WUuY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMxVTzjNPVWjOHUtMzEsOEWRMIQ
WvilIYliVNtK7jTbyB8WUmucwz3JGfP1LZ5AvT5OQsz8tDsILYItGGliC2tcCAwEAAaAXMBUGCSq

```
GSIb3DQEP/LxbucXaasoh0M1TrU/RhjN2wsGVWtKpjnoeXcVZn15OS0adpQtbR4NtmEvL/gXgX+pG
kRImUGzYTjVAMjeau48j4mNW6emf//dWmEHxo2LF2ReHfM3LYM5lh47Wi9Hu/fk87QQTn4lq1aHx
0vyCtlMOlRXdcTptuFywnNTZ1qTctoMbDn+e4M6ILlvyETEnvta0HcMjMOYujNm3SPXOu0shek/Czu
py7srOvMdjV9hmZaGJ2PBpGAfPUqJh5Gb9VOThRbdomlyA==
 -----END CERTIFICATE-----
```

1. Copy and paste the text between the “Begin Certificate” and “End Certificate” delimiters to a text file using a text editor such as Notepad.
2. Save the file on your hard drive and name the file **srv_cert.cer**.
3. On the Viewport **File Transfer** menu, point to **Generate Certificate Request** and then click **Upload Signed Certificate**.
4. Locate the directory where you saved srv_cert.cer and click **Open**. This will upload the signed certificate to the \SYS directory of the 2-Series processor in DER format, i.e., \\sys\srv_cert.der.

### Upload Root Certificate

Along with the signed certificate, all CAs also electronically give access to what is called a **root certificate**. A root certificate is a document that validates the CA itself. At the time of sending the signed certificate, most CAs provide a URL to where their root certificate is stored. The buyer of the signed certificate may then download the root certificate onto the server. Uploading the root certificate is identical to the procedure for uploading signed certificate. The only difference is that the root certificate is stored as: **\\sys\ rootCA_cert.der**.

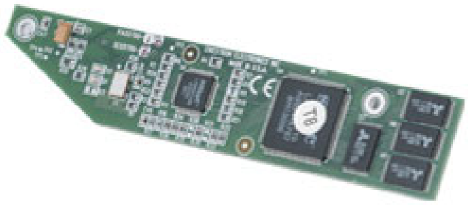
Enable SSL with CA-signed certificate

1. On the Viewport **Functions** menu, click **Set Control System IP Information**.
2. Click the **Advanced** button and click **Enable SSL**.
3. Select **CA-signed** and click **OK** to reboot the control system.

The processor is now SSL protected with a CA-signed certificate. Any Web browser attempting to communicate with the server will display a locked icon on their screen.

## Ethernet Touchpanels

The Crestron TPS-ENET card (shown in the figure) is a Network Interface Card for TPS touchpanels. The card can operate at speeds of 10/100BaseT, and provides half and full duplex capabilities. The TPS-ENET card supports DHCP in addition to static IP addressing.



As with other Crestron units, you use the Viewport to access the panel’s console and set its IP information. The first time you connect to the touchpanel, the connection type must be either Cresnet or RS-232. The exact procedure for establishing communication is described in the documentation for the TPS-ENET card.

Once you connect to the panel, you can set the IP information by typing console commands at the Viewport command prompt.

**For static IP addressing**, the commands are:

- **ADDMASTER <IP ID> < control system address>**: specifies the IP ID of the touchpanel and the static IP address of the master control system(s). TPS touchpanels can accept commands from up to 252 master control systems. (If you are using the Crestron NAT and the touchpanel is located on LAN B, then you type the LAN B address of the control system, not the LAN A address that is visible to the outside network).
- **IPADDRESS <panel address>**: sets the static IP address of the touchpanel.
- **IPMASK <subnet mask address>**: sets the subnet mask.
- **DEFROUTER <default router IP address>**: sets the IP address of the default router.

For example, given the following values:

IP ID 03; IP address 192.168.1.9; subnet mask 255.255.255.0; default gateway address 0.0.0.0; and control system IP address 192.168.1.1

You would type the following at the Viewport command prompt:

```
>ADDMASTER 03 192.168.1.1
>IPADDRESS 192.168.1.9
>IPMASK 255.255.255.0
>DEFROUTER 0.0.0.0
```

**For dynamic IP addressing**, the commands are:

- **ADDMASTER <IP ID> <control system address/FQDN>**: specifies the IP ID of the touchpanel and the static IP address or fully-qualified domain name of the master control system(s). TPS touchpanels can accept commands from up to 252 master control systems.

  (If you are using the Crestron NAT and the touchpanel is located on LAN B, then you type the LAN B address of the control system, not the LAN A address that is visible to the outside network).
- **DHCP ON**: enables DHCP operation.
- **HOSTNAME <name>**: specifies the hostname of the touchpanel.
- **DOMAIN <domain name>** specifies the domain. This command is only necessary if you are configuring DHCP on an Ethernet connection to a touchpanel that currently has a static address. The domain name will be used to reconnect to the touchpanel after it resets. With a serial connection, the domain does not need to be entered.

  Note that the domain supplied by the DHCP server will overwrite the domain indicated here.
- **WINS ON** specifies Windows NT 4.0 Server.
- **WINS OFF** specifies Windows 2000 Server.

## IP Table Setup

The **IP Table** is an internal list that enables the control system to identify and communicate with Crestron Ethernet equipment on an IP network.

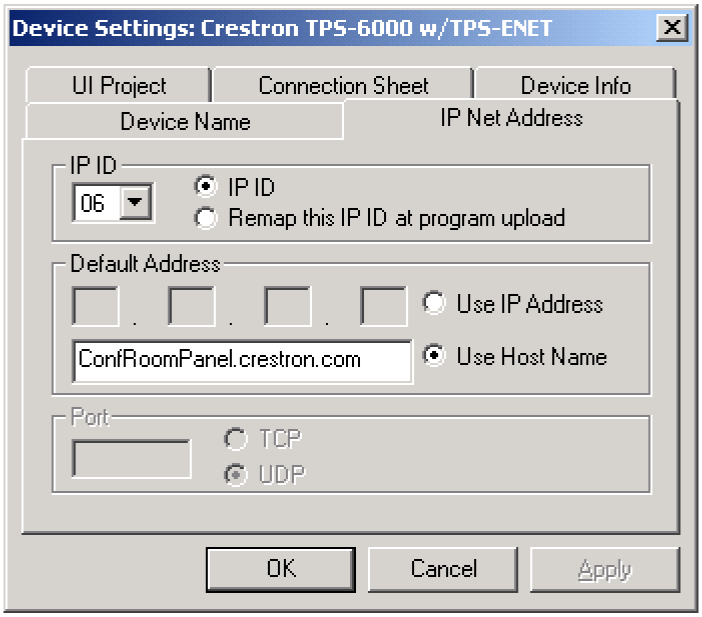
The IP Table consists of each unit's IP address or fully-qualified domain name, together with its IP ID. The IP ID is a hexadecimal value that must be unique and ranges from 03 to FF.

Each controlled Ethernet device also has an IP Table, called a Master List. Here you must set the IP ID of the controlled device and then specify the IP address or FQDN of the control system(s) that will send it commands.

You can enter information into the IP Table in two ways. The first method creates what is referred to as a "default" IP Table, as follows:

1. **For Ethernet Remote Processing and TPS Panels**: Double-click the Ethernet remote processor or TPS panel in the SIMPL™ Windows® Configuration Manager screen to open the **Device Settings** dialog box.
2. Click the **IP Net Address** tab.
3. Click the **IP ID** button and select the hexadecimal IP ID from the list.

   (The "Remap IP ID at program upload" option is reserved for future use.)
4. Click **Use Hostname** and enter the fully-qualified domain name of the remote Ethernet processor or TPS touchpanel.



Device Settings: Crestron TPS-6000 w/TPS-ENET

IP ID: 06

● IP ID

○ Remap this IP ID at program upload

Default Address: ConfRoomPanel.crestron.com

○ Use IP Address

● Use Host Name

Port

○ TCP

● UDP

5. **For Generic Ethernet Modules**: The device settings for Generic Ethernet modules such as the ActiveCNX Interface and e-Control PC Interface are the same regardless of the DHCP setting.

   That is, the IP address should be set to 127.0.0.1 if the internal "hardware" gateway is being used. With the CNX-EGWY, the IP address should be the static IP address of the PC where the gateway resides. (The “Use Hostname” option does not apply.)

The ActiveCNX Interface and e-Control PC Interface are described in detail in the section titled “Interfaces to e-Control”.

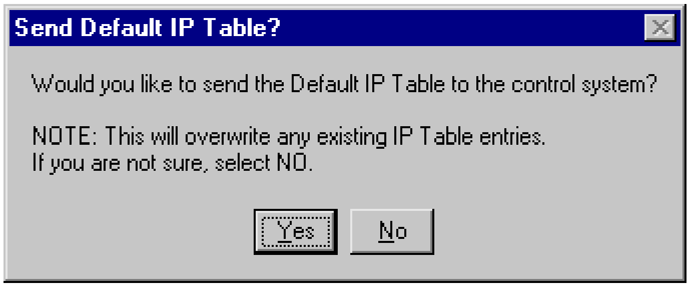
6. **For Ethernet Intersystem Communications**: The configuration settings for the Ethernet ISC symbol depend on the target control system.

    - If the target is enabled for DHCP, then click **Use Hostname** and enter the fully-qualified domain name of the destination control system.
    - If the target is not enabled for DHCP, then click **Use IP Address** and enter the static IP address of the destination control system.

    The Ethernet ISC symbol cannot be used for intersystem communication between an X-Series control system and a DHCP-enabled 2-Series control system.

    The Ethernet ISC symbol is described in detail in the section titled “Interfaces to e-Control”.

7. **With X-Series control systems**, the **Device Settings** dialog box provides a drop-down list for selecting the IP ID, and a text field for entering the static IP address of the controlled device. There is no hostname option.
8. When you upload the completed SIMPL Windows logic program, click **Yes** when prompted to "Send the Default IP Table to the Control System."



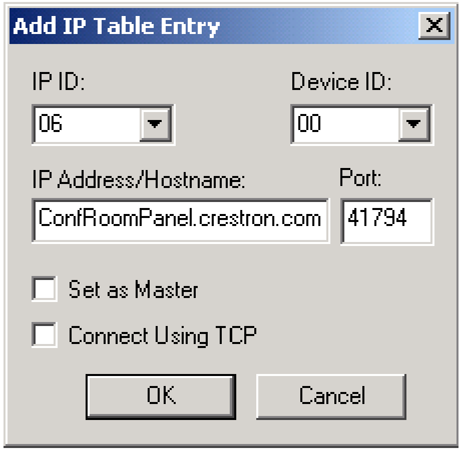
Send Default IP Table?

Would you like to send the Default IP Table to the control system?

NOTE: This will overwrite any existing IP Table entries.
If you are not sure, select NO.

The second method for creating the IP Table enables you to set or change the IP information and send it to the control system without need to re-compile or re-transfer the SIMPL Windows program.

1. Open the Crestron Viewport and select **Setup IP Table** on the **Functions** menu.
2. In **IP Operations**, click **Add** to add the new IP table entry.
3. Select the hexadecimal IP ID of the device from the **IP ID** list.
4. In the **IP Address/Hostname** field, enter the static IP address of the Ethernet device, or if the device is DHCP-enabled, its fully-qualified domain name.



IP ID: 06

Device ID: 00

IP Address/Hostname: ConfRoomPanel.crestron.com

Port: 41794

☐ Set as Master

☐ Connect Using TCP

(The Port field, the "Connect Using TCP" check box and the Device ID list are reserved for future use.)

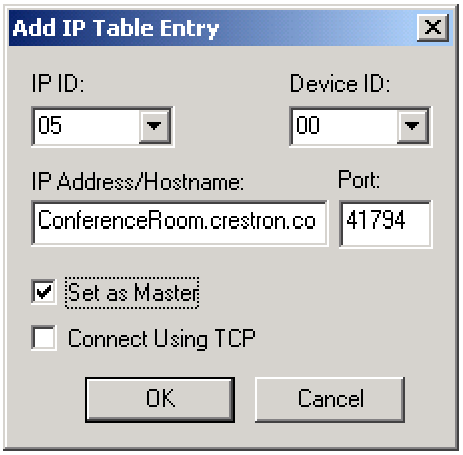
5. When you are satisfied with the IP settings, click **OK** to add the device to the IP Table Editor.
6. Repeat this procedure for all the Ethernet devices in the program. When you are ready to upload, click **Send IP Table to Control System**.

Whenever you send the IP Table to the control system, it will overwrite the previously loaded IP Table.

Each Ethernet device in the SIMPL Windows program also has an IP Table called a **master list**, which sets the device's IP ID and specifies the IP address (or FQDN) of the control system(s) that will send it commands.

**For Remote Ethernet Processing** (2-Series control systems operating in slave mode):

1. Set the IP ID. It must match the IP ID that is listed in the IP Table of the master control system.
2. Enter the IP address or FQDN of the master control system.
3. Select the **Set as Master** check box.



IP ID: 05

Device ID: 00

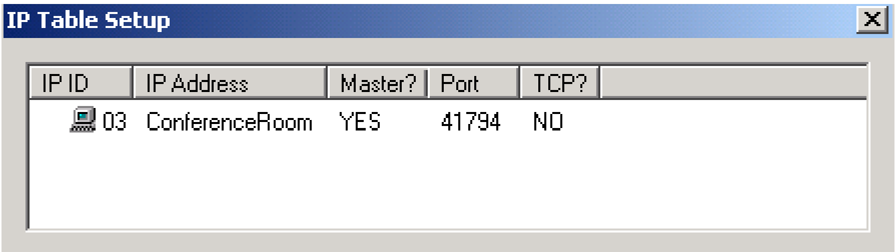
IP Address/Hostname: ConferenceRoom.crestron.co

Port: 41794

☑ Set as Master

☐ Connect Using TCP

When the entry is added to the IP Table editor, the **Master** field will read **YES**.



| IP ID | IP Address | Master? | Port | TCP? |
|---|---|---|---|---|
| 03 | ConferenceRoom | YES | 41794 | NO |

2-Series control systems operating in slave mode can accept commands only from one control system; thus, the IP Table (Master List) will consist of only one entry.

**For the CEN-TVAV**, you also create the IP Table by using the Viewport **Setup IP Table** command. The CEN-TVAV can operate in **mixed mode**, meaning that it can contain its own SIMPL Windows program to control devices, while at the same time operating as a slave device that receives commands from a master control system. The entry for the master control system is the same as described previously:

1. Set the IP ID of the CEN-TVAV, which should match the IP ID that is listed in the IP Table of the master control system.
2. Enter the static IP address of the master control system (CEN devices do not support DHCP).
3. Select the **Set as Master** check box.

The CEN-TVAV can accept commands from only one control system; thus, the IP Table should have only one entry that is "set as master".

**For other CEN devices**, the procedure for setting the IP information differs depending on the device, and is described in each unit's manual. In all cases, however, you must use the Crestron Viewport to access the unit's console. From the console, enter the static IP address, subnet mask and default gateway address. In addition, you must specify the IP ID of the unit, together with the static IP address of the control system(s) that will send it commands.

All the functionality of CEN devices is now also provided by Crestron's 2-Series control systems. When operating in Remote Ethernet Processing mode, a 2-Series processor such as the CP2E provides the same functionality as a CEN-IO, a CEN-COM, a CEN-TVAV, and more, all in one unit.

The table below shows the number of masters each Ethernet device accepts:

| *Ethernet Device* | *Maximum Number of Masters* |
|---|---|
| 2-Series remote processing | 1 |
| CEN-TVAV | 1 |
| CEN-CN | 1 |
| CEN-IO | 5 |
| CEN-COM | 5 |
| TPS Touchpanels | 252 |

## Using the PING Utility to Test an Internet Connection

PING (**P**acket **In**ternet **G**roper) is a utility for testing whether a particular computer or device is connected to the Internet by sending a packet to its IP address and waiting for a response. The PING utility does not use TCP or UDP, but rather it uses another transport-layer protocol called ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol). The purpose of ICMP is to diagnose IP networking issues.

Once you have configured the Crestron equipment, you should “ping” each device to verify the network connection. The PING utility is included with Windows, as well as with Crestron’s 2-Series control systems. To ping a device with Windows, start your Internet connection, open the Windows command prompt and type:

```
ping <IP address or fully-qualified domain name>
```

For example, you can type:

```
ping www.crestron.com or ping 164.109.174.244
```

A good connection will give the following results:

```
Pinging 164.109.174.244 with 32 bytes of data:

Reply from 164.109.174.244: bytes=32 time=260ms TTL=255
Reply from 164.109.174.244: bytes=32 time=221ms TTL=255
Reply from 164.109.174.244: bytes=32 time=190ms TTL=255
Reply from 164.109.174.244: bytes=32 time=180ms TTL=255

Ping statistics for 164.109.174.244:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 180ms, Maximum = 260ms, Average = 212ms
```

No connection will show the following:

```
Pinging 164.109.174.244 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 164.109.174.244:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To use the Crestron Viewport (2-Series processors only), type the ping command at the Viewport command prompt, i.e., **ping 192.168.1.1**. Here a successful connection will show:

```
Remote Node (192.168.1.1) is alive
```

No connection will show the following:

```
Remote Node (192.168.1.1) is not responding
```

### AUTONEGOT Command

As described earlier in this reference guide, Crestron's 2-Series control systems and TPS Ethernet touchpanels have auto-sensing capabilities. That is, the C2ENET and TPS-ENET cards can detect the speed of the Ethernet network and automatically adjust to that speed. This is called **auto-negotiation**, and it is enabled by default. However, if you know the speed of the network and you want to set the speed and duplex type explicitly, you can set these values using the Viewport AUTONEGOT console command.

Here is the syntax of the command:

```
AUTONEGOT <Ethernet Adapter> <ON|10HALF|10FULL|100HALF|100FULL>
```

Where <***Ethernet Adapter***> is 0 for LAN A or 1 for LAN B. "10" and "100" refer to 10Mbps or 100Mbps, and HALF and FULL set the duplex type, as follows:

- 10HALF – auto-negotiation is OFF, use 10Mbps, half duplex.
- 10FULL – auto-negotiation is OFF, use 10Mbps, full duplex.
- 100HALF – auto-negotiation is OFF, use 100Mbps, half duplex.
- 100FULL – auto-negotiation is OFF, use 100Mbps, full duplex.

For example, to set a TPS Ethernet touchpanel to 100 Mbps, full duplex, you type:

```
>AUTONEGOT 0 100FULL
```

## Interfaces to e-Control

The heart of any well-designed control system is the user interface, which provides the link between the end user and the control system. Regardless of how cleverly programmed or sophisticated a given system is, if it lacks a quality user interface it is unlikely to be used to its full potential.

Crestron offers a variety of user interfaces, including Cresnet and TPS touchpanels, wired button panels, keypads, and IR (infrared) and RF (radio frequency) remotes. Any of these interfaces can be used in e-Control.

For example, a Cresnet touchpanel such as a CT-1000 can be used to control Ethernet devices. The control system receives commands from the CT-1000 over Cresnet and forwards the commands over CIP to the device. Feedback from the device is routed by the control system back over Cresnet to the touchpanel. No special programming or IP Table entry is required in SIMPL Windows to use a Cresnet interface in this scenario. That is, the touchpanel symbol detail is defined as usual, with output and feedback signals connected to the inputs and outputs on the controlled device.

When you use a touchpanel as an interface to e-Control (or to any other control method), you design the touch screen pages using Crestron's VisionTools™ Pro-e software (VT Pro-e). The available design options differ depending on the touchpanel. Some panels, like the CT-1000, are referred to as "original" panels. These panels provide basic design options for appearance and feedback. In contrast, Crestron's TPS panels are referred to as "multi-mode". Multi-mode panels are capable of displaying

16-bit color graphics, video and RGB video, sound files, and more. They are called multi-mode because objects in the project can have up to 100 different appearances, or modes, in both their active and inactive states.

In addition to graphics and other static design elements such as borders and lines, VT-Pro-e provides a number of *programmable objects*, including buttons, sliders and gauges. Pages and subpage references are also programmable.

Programmable objects are assigned join numbers that identify digital, analog, and serial inputs and outputs to the touchpanel. When the page design is finished and all join numbers have been assigned to programmable objects, the VT Pro-e project is compiled into a HEX file and uploaded to the touchpanel. All the join numbers in the VT Pro-e project then have to be mapped to inputs and outputs on the touchpanel symbol detail in SIMPL Windows.

## Third-Party Interfaces and the Crestron Gateway

In addition to Crestron user interfaces, users can access the control system with PC-based interfaces such as Web browsers or custom software applications.

Since Internet and PC communication is based on TCP, and Crestron control systems communicate over CIP, these applications require a mechanism called an e-Control **gateway** to translate TCP packets into CIP datagrams, and vice-versa. For example, Web browser commands would be sent over TCP to the e-Control gateway, which would translate the packets into CIP datagrams and forward the data to the control system. The gateway would also translate feedback from the control system and send it back to the browser.

To accommodate the broad range of possible configurations and third-party interfaces, Crestron provides two types of e-Control gateways: an internal "hardware" gateway that is built into the 2-Series processors and the CNXENET+ card; and a licensed software gateway, called the CNX-EGWY, that can be downloaded from the Crestron Web site. In X-Series control systems, the hardware gateway supports up to five simultaneous connections; the 2-Series gateway supports up to 30 connections. The CNX-EGWY can be licensed for any number of simultaneous connections.

The gateway is assigned the IP address of the machine where it resides. This means that if the gateway resides in the control system, its IP address is the same as the control system; if the gateway is located on a PC, then its IP address is the same as the PC.

The term gateway as it is used here should not be confused with the default gateway described before, although both gateways perform a similar function. A default gateway is a router that transfers data from the internal LAN to outside subnets. The Crestron e-Control gateway is software that converts TCP to CIP, and vice versa.

## e-Control Web Pages and e-Control 2

Web pages provide a flexible and inexpensive interface to e-Control, allowing users to control devices on the LAN simply by launching a Web browser on their PC. You can design e-Control Web pages in a number of ways. For software programmers, Crestron includes an SDK (**s**oftware **d**eveloper's **k**it) as part of the CNX-EGWY installation package. The SDK contains Java components and ActiveX controls, routines and documentation for creating custom Web and PC-based interfaces that can communicate with Crestron hardware.

The easiest method, requiring no knowledge of HTML, ActiveX or Java, is to create a Web browser project using VisionTools Pro-e. You design a Web browser project in much the same way as a touchpanel project. When you compile a browser project, VT Pro-e converts the project pages into HTML format. The resulting files are then ready to be uploaded to a Web server.

VT Pro-e provides two options for creating browser projects: one is Java-based, and the other, referred to as “e-Control 2”, is based on Microsoft’s COM technology. With e-Control 2, you also have the option to create a standalone executable that can be launched from the Windows desktop (more on this later). To create a Java-based project, you select **BROWSER** as the “panel type” in VT Pro-e; for a COM-based project (e-Control 2), select **XPANEL**.

Java-based projects require that you license the e-Control portion of VT Pro-e in order to enable the HTML conversion utilities. Crestron e-Control 2 requires that you enable the C2ENET card; you do not have to license VT Pro-e. (Consult the documentation for the C2ENET card for more information on how to enable the card for e-Control 2.)

### *Java-Based Browser Projects*

When you design a Java-based project, each object that you draw on a page is actually a discrete Java *applet*. Applets are small, self-contained programs that can be attached to HTML pages to make them dynamic and interactive.

When you use a Java-enabled Web browser to view a page that contains an applet, that applet's code is transferred to your system and executed by the browser's Java Virtual Machine (JVM). (Crestron distributes a copy of the latest Microsoft JVM with each version of VT Pro-e.) VT Pro-e automatically adds a Java communication component to each Web page when the project is compiled, allowing the Java applets to connect to the e-Control gateway and send and receive digital, analog and serial signals to the control system.

Java-based projects require special design considerations because of the overhead incurred by transferring Java applets each time a page is loaded or refreshed. For example, to reduce download time, the Web pages should be as simple and uncluttered as possible, with a minimum number of graphics. In addition, subpages should be used sparingly, if at all. Subpages are opened in a new browser window that the user can resize or reposition, which can lead to undesirable results.

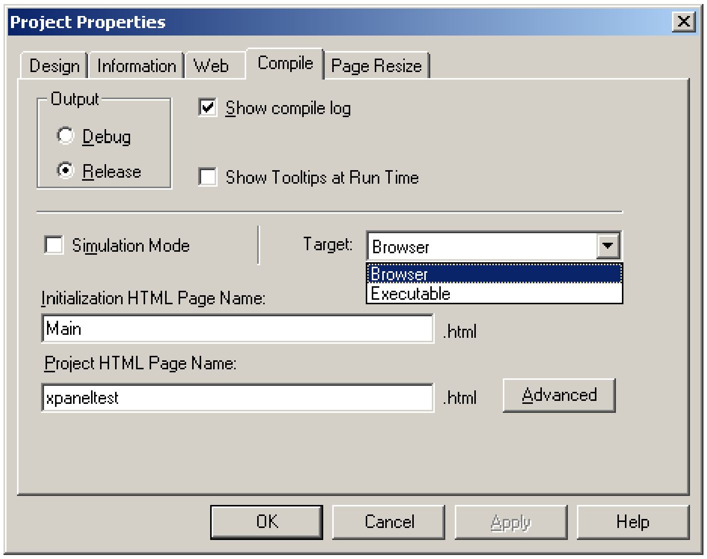
Finally, you need to test projects with Web browsers such as Netscape Navigator, since the page display and layout can vary widely depending on the JVM. For example, layered objects, which are commonly used in VT Pro-e projects, may look and behave differently depending on the browser.

### *XPANEL Projects (e-Control 2)*

The purpose of e-Control 2 is to give e-Control Web pages (or standalone executables) the same look and feel as TPS touchpanel pages, with almost none of the overhead associated with Java-based projects. Crestron e-Control 2 uses industry-standard COM technology designed specifically for Microsoft Internet Explorer and Windows.

XPANEL projects differ from Java-based projects in several important ways. First, XPANEL projects are multi-mode, allowing you to make full use of the same design elements and features available for TPS panels. Unlike Java-based projects, you can readily convert existing touchpanel projects to e-Control 2. In addition, subpages will appear just as they do in touchpanel projects, and the appearance of layered objects will always be consistent.

When you compile a Java-based project, VT Pro-e generates one HTML file for each page in the project. With e-Control 2, only two HTML files are generated: an initialization file that optimizes the download process and ensures that only the latest components are installed; and a project file containing the HTML user interface. Once the project file is downloaded, no further page updates are necessary, meaning that the run-time performance will be the same as with a touchpanel.



Output: ○ Debug ● Release

☑ Show compile log

□ Show Tooltips at Run Time

□ Simulation Mode

Target: Browser (Browser, Executable)

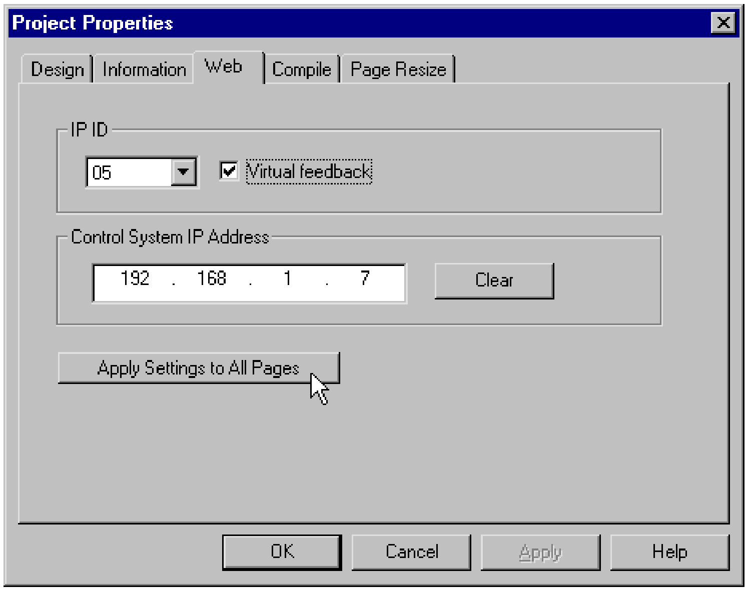
Initialization HTML Page Name: Main .html

Project HTML Page Name: xpaneltest .html

To create an XPANEL project, simply select **XPANEL** as the panel type in VT Pro-e. Then click **Project Properties** on the **Edit** menu. Go to the **Compile** tab and select **Browser** as the target, as shown in the diagram. You can change the filenames of the initialization and project files by entering new names in the .html text fields.

### *IP Settings (Java and XPANEL)*

Like other components of e-Control, the pages in a browser project must be assigned an IP ID. In most cases, you can give all the pages in the project the same IP ID: go to the **Web** tab of the **Project Properties** dialog box. Select the IP ID from the drop-down list, and enter the IP address or fully-qualified domain name of the control system.



IP ID: 05 ☑ Virtual feedback

Control System IP Address: 192 . 168 . 1 . 7

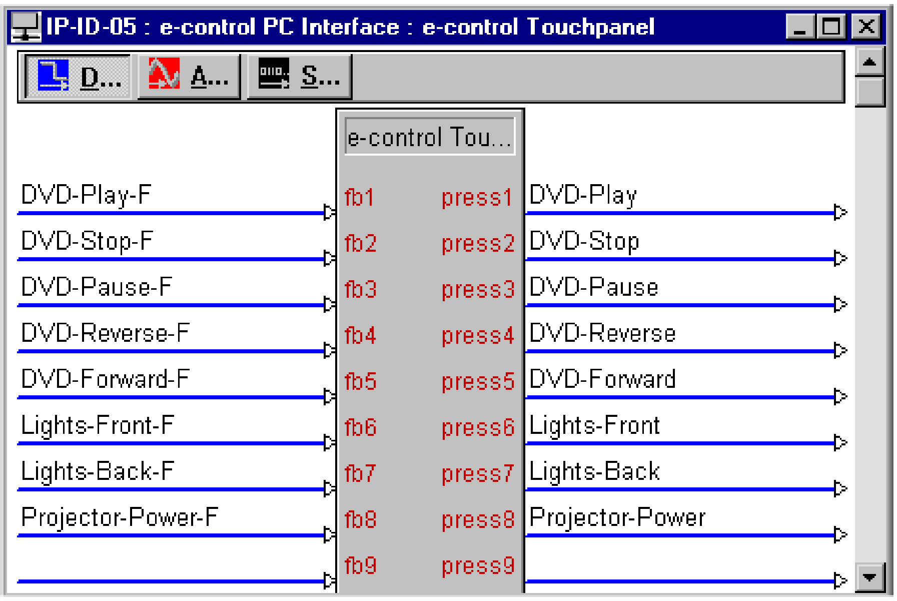
As shown in the previous diagram, you can click **Apply Settings to All Pages** to set the same IP information to all the pages in the browser project. You can also click the **Virtual feedback** check box if you want to enable “instant” feedback. This feature causes an object such as a button to display in its active state the moment the user clicks it, even if there is some delay in receiving actual feedback from the controlled device.

### *SIMPL Windows Programming (Java and XPANEL)*

For each IP ID you set in the VT Pro-e browser project, you must define one *e-Control PC Interface* symbol in the SIMPL Windows program. (If you assign the same IP ID to all the pages in the browser project, you need to define just one PC Interface symbol.) The PC Interface symbol is located in the Ethernet Modules folder of the Device Library and the symbol detail is defined identically to a touchpanel symbol. That is, all the join numbers you define in the VT Pro-e project map to signals on the symbol detail.

To configure the symbol, open the SIMPL Windows Configuration Manager screen:

1. Drag the e-Control PC Interface symbol from the Device Library to the Ethernet slot on the control system. Double-click the symbol to open the **Device Settings** dialog box.
2. Click the **IP Net Address** tab and select the same IP ID that was set for the HTML pages in the VT Pro-e browser project. Then enter the IP address of the machine where the e-Control gateway resides. If the gateway is the internal “hardware” gateway, the IP address is 127.0.0.1. If the gateway is the CNX-EGWY, the IP address is the address of the PC.
3. When you bring the PC Interface symbol to *Detail View* in Program Manager, you have to map the previously defined join numbers to inputs and outputs on the symbol.



| Input signal | Input | Output | Output signal |
|---|---|---|---|
| DVD-Play-F | fb1 | press1 | DVD-Play |
| DVD-Stop-F | fb2 | press2 | DVD-Stop |
| DVD-Pause-F | fb3 | press3 | DVD-Pause |
| DVD-Reverse-F | fb4 | press4 | DVD-Reverse |
| DVD-Forward-F | fb5 | press5 | DVD-Forward |
| Lights-Front-F | fb6 | press6 | Lights-Front |
| Lights-Back-F | fb7 | press7 | Lights-Back |
| Projector-Power-F | fb8 | press8 | Projector-Power |
|  | fb9 | press9 |  |

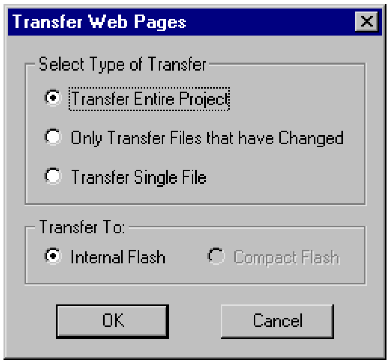
Once the Web browser establishes a TCP/IP connection to the e-Control gateway, data can pass back and forth between the browser and the control system, just as with any other interface. The gateway receives commands from the browser over TCP, performs the translation to CIP and forwards the data to the control system. Feedback from the control system is routed back by the gateway to the Web browser.

The control system cannot initiate communication with a Web browser; it can only listen for a connection.

### *Uploading HTML Pages to a Web Server*

Once you have created the e-Control Web pages with either VT Pro-e or the Crestron SDK, you are ready to upload them to a Web server. The procedure differs depending on the location of the Web server. If you are using the Web server that is built into the 2-Series processor or CNXENET+ card, you can use the Crestron Viewport. You can also use the Viewport to upload Web pages to Compact Flash (for 2-Series only):

1. From the Viewport **File Transfer** menu, click **Send Web Pages**. The options are to send an entire project, only files that have changed, or a single HTML file. With a 2-Series control system, select the target: Internal Flash or Compact Flash.



Transfer Web Pages

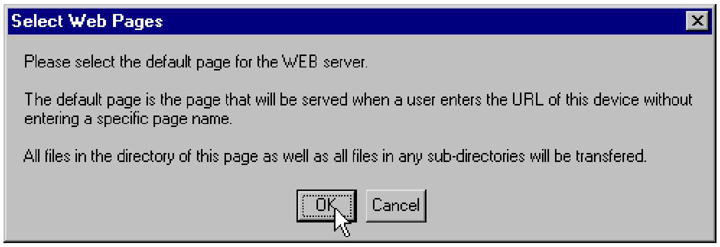
Select Type of Transfer

● Transfer Entire Project
○ Only Transfer Files that have Changed
○ Transfer Single File

Transfer To:

● Internal Flash ○ Compact Flash

With the **Transfer Entire Project** option, click **OK** when reminded to select the default page. This is the first page that will be displayed when the user connects to the server.



Select Web Pages

Please select the default page for the WEB server.

The default page is the page that will be served when a user enters the URL of this device without entering a specific page name.

All files in the directory of this page as well as all files in any sub-directories will be transfered.

2. Locate the directory containing the HTML files. Select the default page, click **Open**, and then click **OK** to begin the transfer. As indicated in the previous diagram, the default page will be uploaded along with all the other files in the same directory, including all subdirectories.

   With a Java-based project, the default page should be the page you “mark as first" in VT Pro-e. With an XPANEL project, select the initialization file as the default.

If you change any of the HTML files in your project, the changed files can be transferred without need to resend the entire project. Simply choose the **Only Transfer Files that have Changed** option. Here again, you select the default page, click **Open**, and then **OK** to transfer the changed files.

During transfer, Viewport compares the files in the HTML project folder with those that currently exist on the Web server. If the Web server contains any files that are not present in the project, those files will be deleted from the Web server.

Finally, you can send a single HTML page by selecting **Transfer Single File**. Locate the file and click **Open**. Then specify the file's relative path (from the root directory) and click **OK**. Note that this will delete any other pages that are present in the Web server.

*Compact Flash Feature*

As just described, you can use the Viewport to transfer e-Control Web pages to Compact Flash, rather than to internal memory on the 2-Series processor. In addition, if you have a Compact Flash reader/writer drive on your PC, you can load HTML pages to a Compact Flash card using Windows Explorer or any other file transfer method. The files should be saved in a directory called **HTML**.

When you insert the card into the Memory Expansion slot of the control system, the control system will look for the HTML directory and automatically load the Web pages to the Web server. (The **HTML** directory must also include a configuration file called config_ini, which identifies the default page.)

### Standalone Executables

In addition to generating Web pages, e-Control 2 can generate a standalone program that can run on any Windows PC. This is an ideal option if the system will not be accessed by a large number of dynamically assigned clients, but rather by a few static computers. This scenario does not require a server to deliver the e-Control 2 pages. All the data can be stored locally on the Windows PC.

You can design and create a standalone executable just as you would an e-Control 2 browser project:

1. Select **XPANEL** as the panel type in VT Pro-e.
2. In **Project Properties**, go to the **Compile** tab and select **Executable** as the target.
3. Go to the **Web** tab and assign an IP ID to all the project pages. Then specify the IP address or fully-qualified domain name of the control system.

On the SIMPL Windows side, programming is the same as with a browser project:

- Map the join numbers in the VT Pro-e project to inputs and outputs on the e-Control PC Interface symbol detail, as described before.
- The e-Control PC Interface symbol should be assigned the IP ID of the project pages as assigned in VT Pro-e, together with the IP address of the gateway. Note that you do not have to install the licensed CNX Gateway for a

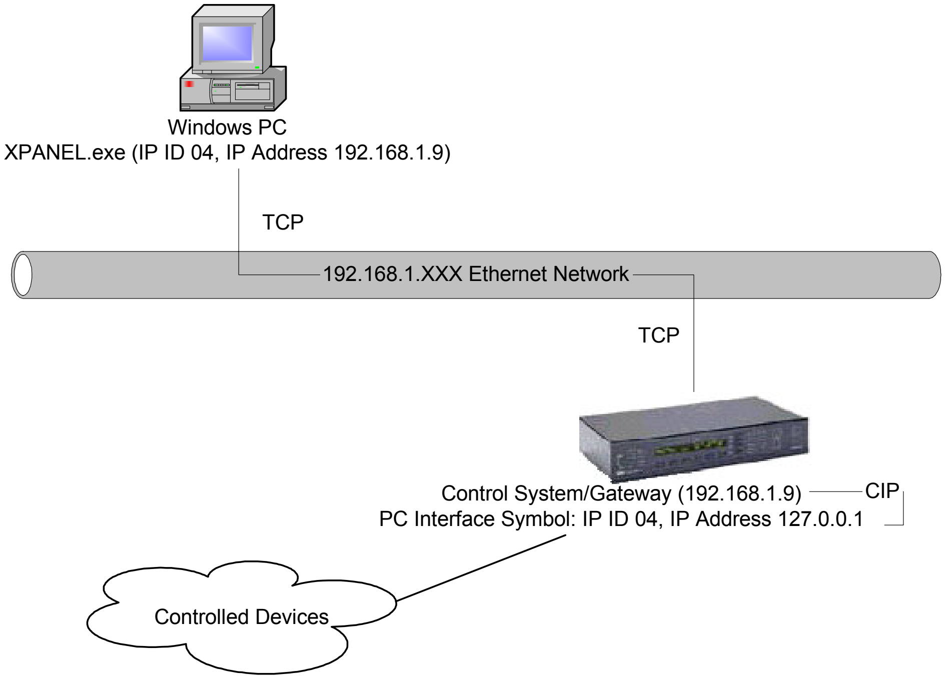
standalone executable. Use the control system's built-in "hardware" gateway (127.0.0.1).

When you compile the project, VT Pro-e will generates an .exe program file and other associated files and saves them in a folder with the project name and an .xexe extension. You have to transfer this folder and all its contents to the user's machine. You can save the XEXE folder in any directory, and you can create a shortcut to the EXE file from the Windows desktop, as you would with any program.

After you transfer the program files, launch the executable on the user's machine. This will open the e-Control 2 screen and display the message: "The connection to hardware was not established." Click **Settings** on the **Options** menu and enter the IP address or fully-qualified domain name of the control system. Then refresh the page by clicking **Restart** on the **File** menu, or pressing the F5 key.

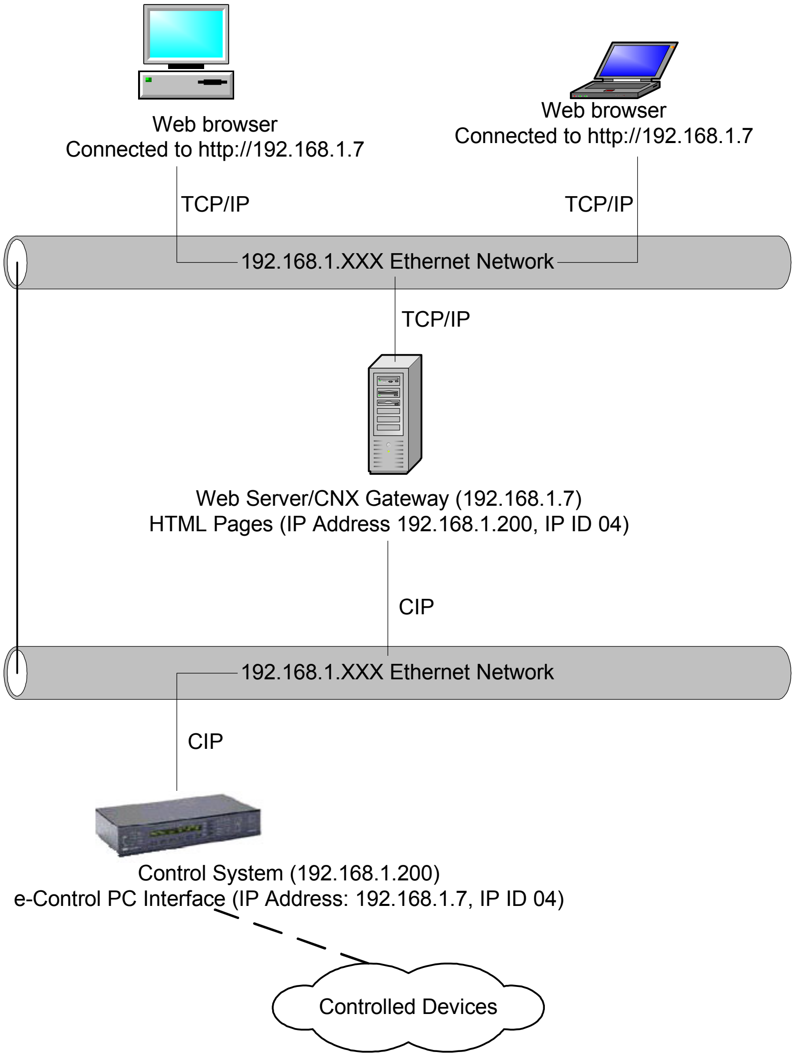
### *Gateway Configurations*

In the configuration shown below, the PC containing the standalone executable connects to the "hardware" gateway that is built into the 2-Series processor. This scenario does not require the licensed CNX-EGWY.

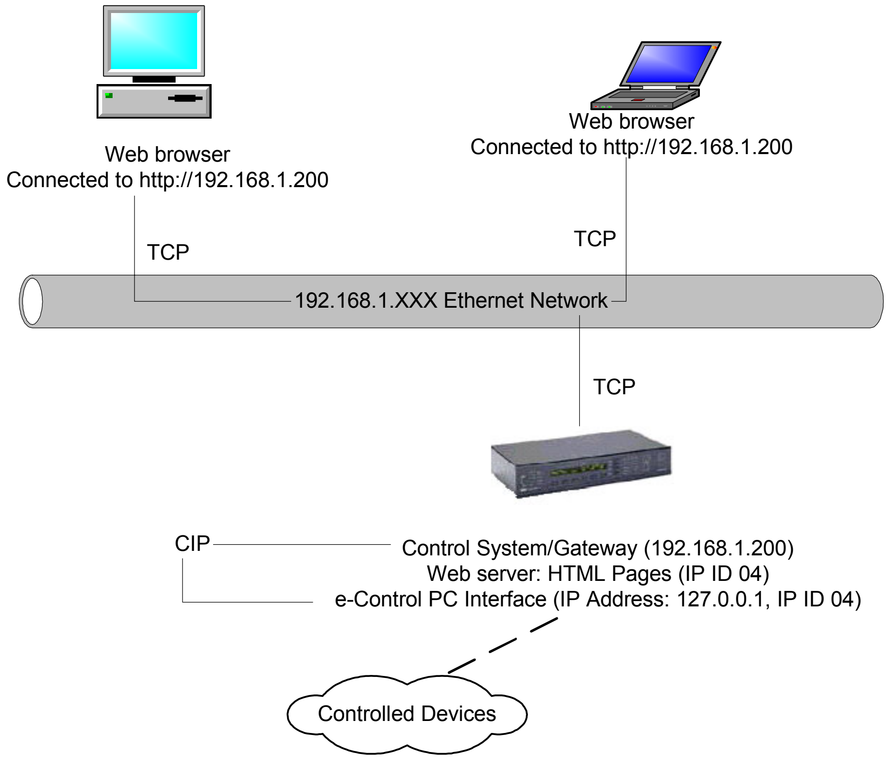

Windows PC
XPANEL.exe (IP ID 04, IP Address 192.168.1.9)
TCP
192.168.1.XXX Ethernet Network
TCP
Control System/Gateway (192.168.1.9)
PC Interface Symbol: IP ID 04, IP Address 127.0.0.1
CIP
Controlled Devices

Two gateway configurations enable a Web browser to access the control system. In both cases, the e-Control gateway must reside on the same machine as the Web server containing the HTML pages. This applies to both Java-based and e-Control 2 pages.

In the configuration shown below, the Web server and CNX-EGWY are located outside the control system. Each Web browser initiates a connection to the gateway. This configuration supports however many connections for which the CNX-EGWY is licensed.


Web browser
Connected to http://192.168.1.7
Web browser
Connected to http://192.168.1.7
TCP/IP
TCP/IP
192.168.1.XXX Ethernet Network
TCP/IP
Web Server/CNX Gateway (192.168.1.7)
HTML Pages (IP Address 192.168.1.200, IP ID 04)
CIP
192.168.1.XXX Ethernet Network
CIP
Control System (192.168.1.200)
e-Control PC Interface (IP Address: 192.168.1.7, IP ID 04)
Controlled Devices

The configuration shown below uses the “hardware” gateway that is built into the 2-Series control processor; the Web pages are stored in the control system’s internal Web server. This configuration supports a maximum of 30 simultaneous connections. (The CNXENET+ card supports up to five simultaneous connections.)


Web browser
Connected to http://192.168.1.200
Web browser
Connected to http://192.168.1.200
TCP
TCP
192.168.1.XXX Ethernet Network
TCP
CIP
Control System/Gateway (192.168.1.200)
Web server: HTML Pages (IP ID 04)
e-Control PC Interface (IP Address: 127.0.0.1, IP ID 04)
Controlled Devices

## ActiveCNX

ActiveX controls are special “applications”, similar to Java applets, which can be plugged into Web pages or other PC-based programs to extend functionality. They are designed to be small, precompiled, modular and reusable. Microsoft, as well as hundreds of third-party developers, create and market ActiveX controls. Many software development tools support ActiveX controls, including Visual Basic, Visual C++, PowerBuilder, Java, and Delphi, so that most programmers can create ActiveX controls if their application warrants it.

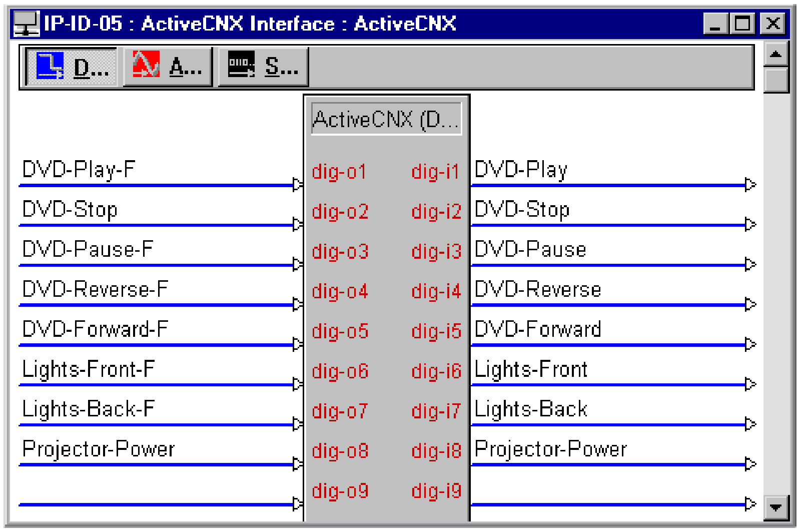
Crestron developed its own ActiveX control, called *ActiveCNX*, to enable any software program that supports ActiveX technology to be used as an interface to e-Control. Crestron also incorporates ActiveCNX in its e-Control Power Applications, such as e-Outlook and e-PowerPoint. The control, together with its routines and documentation, are contained in the Crestron SDK.

Like Crestron’s Java components, an ActiveCNX control has the capability to connect to the e-Control gateway; send and receive digital, analog, and serial signals, using the same “join number” scheme as a touchpanel.

Each ActiveCNX control in a PC application must have a corresponding *ActiveCNX Interface* symbol defined in the SIMPL Windows program. The ActiveCNX Interface symbol is found in the Ethernet Modules folder of the Device Library. It must be assigned an IP ID and IP address; both the IP ID and IP address must be entered into the IP Table of the control system.

The Ethernet Modules folder also includes interface symbols for Crestron’s e-Control Power Applications; for example, there’s an e-PowerPoint Interface and an e-Outlook Interface. All of these symbols are based on the ActiveCNX Interface symbol.

The ActiveCNX Interface symbol detail is defined in the same way as a touchpanel. That is, join numbers defined in the ActiveCNX control are mapped to signals on the symbol. The signals on the output side trigger actions or other logic in the program, while the signals on the input side can be sent as feedback to the ActiveCNX control.



IP-ID-05 : ActiveCNX Interface : ActiveCNX

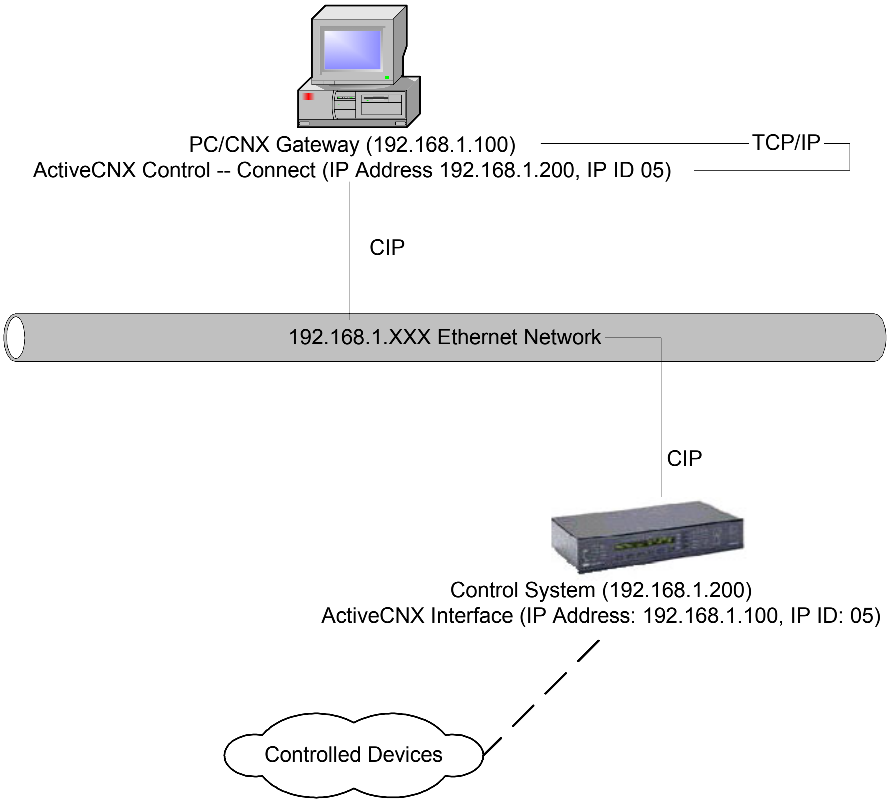
|  | ActiveCNX (D... |  |  |
|---|---|---|---|
| DVD-Play-F | dig-o1 | dig-i1 | DVD-Play |
| DVD-Stop | dig-o2 | dig-i2 | DVD-Stop |
| DVD-Pause-F | dig-o3 | dig-i3 | DVD-Pause |
| DVD-Reverse-F | dig-o4 | dig-i4 | DVD-Reverse |
| DVD-Forward-F | dig-o5 | dig-i5 | DVD-Forward |
| Lights-Front-F | dig-o6 | dig-i6 | Lights-Front |
| Lights-Back-F | dig-o7 | dig-i7 | Lights-Back |
| Projector-Power | dig-o8 | dig-i8 | Projector-Power |
|  | dig-o9 | dig-i9 |  |

The Active CNX control initiates a connection to the control system—and its associated ActiveCNX Interface symbol—through a method, or internal command, called Connect( ). This method has two parameters: 1) The IP address or fully-qualified domain name of the control system; and 2) The IP ID of the ActiveCNX Interface symbol, as set in SIMPL Windows.

On the control system (SIMPL Windows) side, the ActiveCNX Interface symbol is assigned the IP address of the machine where the gateway resides, and an IP ID that matches what is passed to the Connect( ) method.

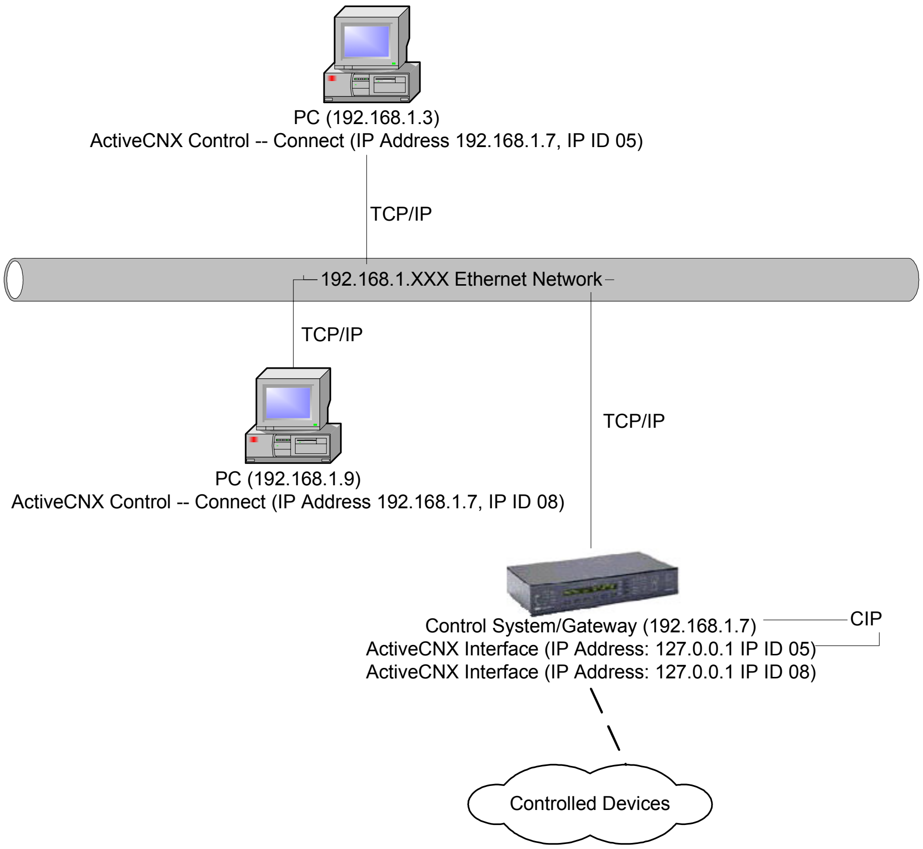
The control system functions as a server; it cannot initiate a connection to the ActiveCNX control. It can only listen for a connection. The ActiveCNX control acts as a client; it initiates the connection.

In the configuration shown below, the ActiveCNX control resides on the same PC as the CNX-EGWY. Here the ActiveCNX control uses the Connect( ) command to start the connection, while the gateway receives the TCP/IP packet and converts it to a CIP datagram. The data is forwarded to the control system.

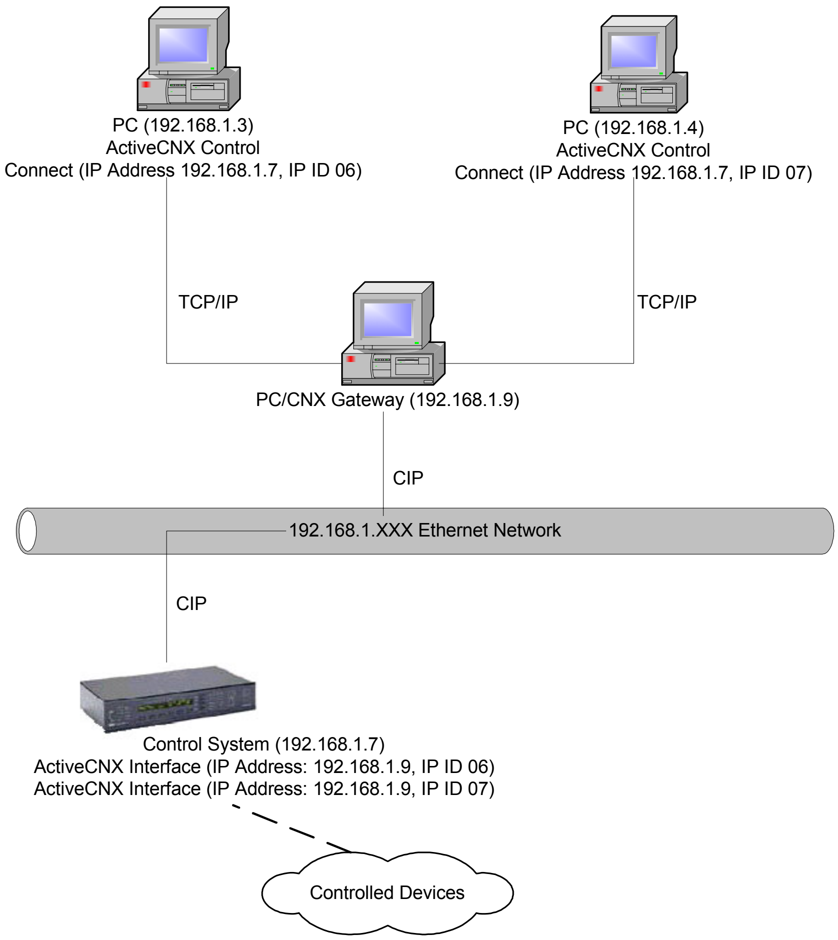

PC/CNX Gateway (192.168.1.100)
ActiveCNX Control -- Connect (IP Address 192.168.1.200, IP ID 05)
TCP/IP
CIP
192.168.1.XXX Ethernet Network
CIP
Control System (192.168.1.200)
ActiveCNX Interface (IP Address: 192.168.1.100, IP ID: 05)
Controlled Devices

Once a connection is established, data can pass back and forth between the PC application and the control system, just as with any other interface. As commands are sent to the control system, the control system forwards the commands to controlled devices. Feedback from the devices is sent to the control system and goes back in real time to the PC application.

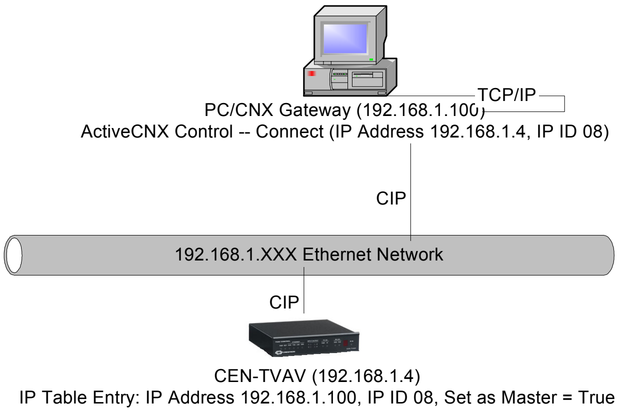
Other configurations are possible. In the setup shown below, the gateway is the “hardware” gateway that is built into the Ethernet card on the control system. Here each ActiveCNX control calls the Connect( ) method to start a TCP/IP connection to the control system. The e-Control gateway receives the packets and performs the translation to CIP.


PC (192.168.1.3)
ActiveCNX Control -- Connect (IP Address 192.168.1.7, IP ID 05)
TCP/IP
192.168.1.XXX Ethernet Network
TCP/IP
PC (192.168.1.9)
ActiveCNX Control -- Connect (IP Address 192.168.1.7, IP ID 08)
TCP/IP
Control System/Gateway (192.168.1.7)
ActiveCNX Interface (IP Address: 127.0.0.1 IP ID 05)
ActiveCNX Interface (IP Address: 127.0.0.1 IP ID 08)
CIP
Controlled Devices

In the configuration shown below, the CNX-EGWY resides on a PC that acts as a server to the other PCs.


PC (192.168.1.3)
ActiveCNX Control
Connect (IP Address 192.168.1.7, IP ID 06)
PC (192.168.1.4)
ActiveCNX Control
Connect (IP Address 192.168.1.7, IP ID 07)
TCP/IP
TCP/IP
PC/CNX Gateway (192.168.1.9)
CIP
192.168.1.XXX Ethernet Network
CIP
Control System (192.168.1.7)
ActiveCNX Interface (IP Address: 192.168.1.9, IP ID 06)
ActiveCNX Interface (IP Address: 192.168.1.9, IP ID 07)
Controlled Devices

The ActiveCNX control can also communicate directly with a CEN device. In this configuration, the CNX-EGWY is required, since the CEN device does not provide an internal "hardware" gateway.


TCP/IP
PC/CNX Gateway (192.168.1.100)
ActiveCNX Control -- Connect (IP Address 192.168.1.4, IP ID 08)
CIP
192.168.1.XXX Ethernet Network
CIP
CEN-TVAV (192.168.1.4)
IP Table Entry: IP Address 192.168.1.100, IP ID 08, Set as Master = True

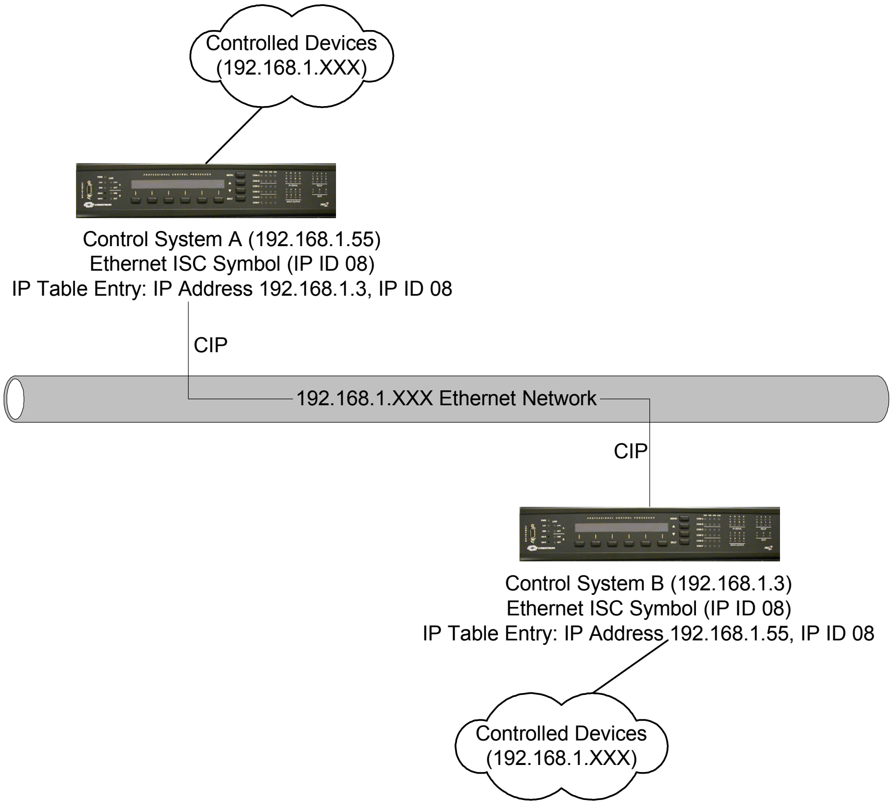
## Intersystem Communication

The Ethernet Intersystem Communications symbol (Ethernet ISC) allows two control systems to exchange information over Ethernet. The ISC symbol takes its digital, analog and serial inputs and converts them into packets for transmission on the Ethernet network. At the destination control system, a matching ISC symbol receives the packets and drives its outputs to the corresponding values. In this way, the inputs of one symbol drive the outputs of the other symbol, and vice versa.

As with all other Ethernet devices, each Ethernet ISC symbol must have an entry in the IP Table of each control system. Here the IP IDs of both Ethernet ISC symbols must be the same. In addition, each symbol must be assigned the IP address or fully-qualified domain name of the *target* control system. That is, in System A, an Ethernet ISC symbol with IP ID 08 would be assigned the IP address or FQDN of System B. The Ethernet ISC symbol in System B would likewise have IP ID 08, and be assigned the IP address or FQDN of System A.

Note that there can be as many Ethernet ISC symbols in a control system as there are available IP IDs (maximum of 251), and thus many communication channels can be established between control systems.

The Ethernet ISC symbol cannot be used for intersystem communication between an X-Series control system and a DHCP-enabled 2-Series control system.


Controlled Devices
(192.168.1.XXX)
Control System A (192.168.1.55)
Ethernet ISC Symbol (IP ID 08)
IP Table Entry: IP Address 192.168.1.3, IP ID 08
CIP
192.168.1.XXX Ethernet Network
CIP
Control System B (192.168.1.3)
Ethernet ISC Symbol (IP ID 08)
IP Table Entry: IP Address 192.168.1.55, IP ID 08
Controlled Devices
(192.168.1.XXX)

# Appendix A: Glossary

**10BaseT** - An Ethernet standard that uses twisted wire pairs.

**100BaseTX** - IEEE physical layer specification for 100 Mbps over two pairs of Category 5 UTP or STP wire.

**1000BASE-T -** Provides half-duplex (CSMA/CD) and full-duplex 1000 Mbps Ethernet service over Category 5 links as defined by ANSI/TIA/EIA-568-A. Topology rules for 1000BASE-T are the same as those used for 100BASE-T. Category 5 link lengths are limited to 100 meters by the ANSI/TIA/EIA-568-A cabling standard. Only one CSMA/CD repeater will be allowed in a collision domain.

**Adapter -** Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card (NIC) is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

**Auto-negotiate** - The term is used to automatically determine the correct settings. It is often used with communications and networking. For example, Ethernet 10/100 cards, hubs, and switches can determine the highest speed of the node they are connected to and adjust their transmission rate accordingly.

**Backbone** – The part of a network that connects most of the systems and networks together and handles the most data.

**Bandwidth** - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

**Bit** – A binary digit. The value—0 or 1—used in the binary numbering system. Also, the smallest form of data.

**Boot** – To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it, and pass control to it.

**Bottleneck** – A traffic slowdown that results when too many network nodes try to access a single node, often a server node, at once.

**Bridge** - A device that interconnects different networks together.

**Broadband -** A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data, and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

**Browser** - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

**Cable Modem -** A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

**CAT 5** - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify “categories” (the singular is commonly referred to as “CAT”) of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

**CAT 5e** - The additional cabling performance parameters of return loss and far end crosstalk (FEXT) specified for 1000BASE-T and not specified for 10BASE-T and 100BASE-TX are related to differences in the signaling implementation. 10BASE-T and 100BASE-TX signaling is unidirectional—signals are transmitted in one direction on a single wire pair. In contrast, Gigabit Ethernet is bi-directional—signals are transmitted simultaneously in both directions on the same wire pair; that is, both the transmit and receive pair occupy the same wire pair.

**CPU** (**C**entral **P**rocessing **U**nit) - The computing part of the computer. Also called the “processor,” it is made up of the control unit and ALU.

**CSMA/CD** (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection) - The LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and each waits a random amount of time before retrying.

**Daisy Chain** - Connected in series, one after the other. Transmitted signals go to the first device, then to the second, and so on.

**Database** - A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

**Data Packet** - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

**Default Gateway** - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

**DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet’s set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a “lease” or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It’s especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

**DMZ** - (**D**e**M**ilitarized **Z**one) allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

**DNS** - The Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address. Every domain has a domain name server that responds to each request. Requests originate from programs and other name servers. Either way, the server converts domain names into IP addresses if the request is accepted. If the request is not accepted, the name server can contact other name servers, offer the IP address for a name server that might complete the request, or return an error message stating that the requested domain name is invalid or does not exist.

**Domain** - A sub-network comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

**Download** - To receive a file transmitted over a network. In a communications session, download means receive, and upload means transmit.

**Driver** - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

**Dynamic IP Address** - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

**Dynamic Routing** - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

**Ethernet** - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

**Fast Ethernet** - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

**Firewall** - A firewall is a set of related programs, located at a network gateway server, which protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

A firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

**Firmware** - Programming that is inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

**Fragmentation** - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

**FTP** (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the Web server using FTP.

FTP includes functions to log onto the network, list directories, and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be “attached,” FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

**Full Duplex** - The ability of a device or line to transmit data simultaneously in both directions.

**Gateway** – A device that interconnects networks with different, incompatible communications protocols.

**Half Duplex** - Data transmission that can occur in two directions over a single line, but only one direction at a time.

**Hardware** - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the “box” and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

**Hub** - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

**IEEE** - The Institute of Electrical and Electronics Engineers. The IEEE describes itself as “the world's largest technical professional society—promoting the development and application of electro technology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.”

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and has several large societies in special areas, such as the IEEE Computer Society.

**IP Address** - In the most widely installed level of the Internet Protocol (Internet Protocol) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required). The message is sent to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address of the note’s recipient. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

**IPCONFIG** - A utility that provides for querying, defining and managing IP addresses within a network. A common Windows NT/2000 utility. It is used for configuring networks with static IP addresses.

**IPSec** - IPSec (**I**nternet **P**rotocol **Sec**urity) is a developing standard for security at the network or packet-processing layer of network communication. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

**IRQ** (**I**nterrupt **R**e**Q**uest) - A hardware interrupt on a PC. There are 16 IRQ lines used to signal the CPU that a peripheral event has started or terminated. Except for PCI devices, two devices cannot use the same line.

**ISP** - An ISP (Internet service provider) is a company that provides individuals and companies access to the Internet and other related services such as website building and virtual hosting.

**LAN** - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

**Latency** - The time delay between when the first bit of a packet is received and the last bit is forwarded.

**MAC Address** - The MAC (Media Access Control) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

**Mbps** (**M**ega**B**its **P**er **S**econd) - One million bits per second; unit of measurement for data transmission.

**Motherboard** - A motherboard is the physical arrangement in a computer that contains the computer's basic circuitry and components.

**NAT** - NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

**NetBEUI** (**NetB**IOS **E**xtended **U**ser **I**nterface) - The transport layer for NetBIOS. NetBIOS and NetBEUI were originally part of a single protocol suite that was later separated. NetBIOS sessions can be transported over NetBEUI, TCP/IP, and SPX/IPX protocols.

**NetBIOS** - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

**Network** - A system that transmits any combination of voice, video, and/or data between users.

**Network Mask** - also known as the "Subnet Mask."

**NIC** (**N**etwork **I**nterface **C**ard) - A board installed in a computer system, usually a PC, to provide network communication capabilities to and from that computer system. Also called an adapter.

**Notebook (PC)** - A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, at temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

**Packet Filtering** - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

**Partitioning** - To divide a resource or application into smaller pieces.

**PCI** (**P**eripheral **C**omponent **I**nterconnect) - A peripheral bus commonly used in PCs, Macintoshes and workstations. It was designed primarily by Intel and first appeared on PCs in late 1993. PCI provides a high-speed data path between the CPU and peripheral devices (video, disk, network, etc.). There are typically three or four PCI slots on the motherboard. In a Pentium PC, there is generally a mix of PCI and ISA slots or PCI and EISA slots. Early on, the PCI bus was known as a "local bus."

PCI provides "plug and play" capability, automatically configuring the PCI cards at startup. When PCI is used with the ISA bus, the only thing that is generally required is to indicate in the CMOS memory, which IRQs are already in use by ISA cards. PCI takes care of the rest.

PCI allows IRQs to be shared, which helps to solve the problem of limited IRQs available on a PC. For example, if there were only one IRQ left over after ISA devices were given their required IRQs, all PCI devices could share it. In a PCI-only machine, there cannot be insufficient IRQs, as all can be shared.

**PCMCIA** - The PCMCIA (Personal Computer Memory Card International Association) is an industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer.

**Ping** (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

**Plug-and-Play** - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

**Port** - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems, and printers.

**Port Mirroring** - Port mirroring, also known as a roving analysis port, is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely.

**PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A method used mostly by DSL providers for connecting personal computers to a broadband modem for Internet access. It is similar to how a dial-up connection works but at higher speeds and quicker access.

**PPTP** (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

**PrintServer** - A hardware device that enables a printer to be located anywhere in the network.

**RIP** (**R**outing **I**nformation **P**rotocol) **-** A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers. It is known to waste bandwidth. AppleTalk, DECnet, TCP/IP, NetWare, and VINES all use incompatible versions of RIP.

**RJ-11** (**R**egistered **J**ack-**11**) - A telephone connector that holds up to six wires. The RJ-11 is the common connector used to plug a telephone into a wall. (The 6-position cable is also known by some as a RJ-12.)

**RJ-45** - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

**Router** - Protocol-dependent device that connects sub networks together. Routers are useful in breaking down a very large network into smaller sub networks; they introduce longer delays and typically have much lower throughput rates than bridges.

**SOHO** (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

**Static IP Address -** A permanent IP address that is assigned to a node in a TCP/IP network.

**Static Routing** - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

**Storage** - The semi-permanent or permanent holding place for digital data.

**STP** (**S**hielded **T**wisted **P**air) - Telephone wire that is wrapped in a metal sheath to eliminate external interference.

**Subnet Mask** - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

**Swapping** - Replacing one segment of a program in memory with another and restoring it back to the original when required.

**Switch** – 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

**Server** - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

**Software** - Instructions for the computer. A series of instructions that performs a particular task is called a “program.” The two major categories of software are application software and system software. Application software is the program of interest that enables users to complete specific tasks. System software includes operating systems and any program that supports application software.

**TCP** (**T**ransmission **C**ontrol **P**rotocol) - A method (protocol) used along with the Internet Protocol (Internet Protocol) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

**TCP/IP** - Transmission Control Protocol/Internet Protocol (TCP/IP) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

**TFTP** (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

**Throughput** - The amount of data moved successfully from one place to another in a given time period.

**Topology** - A network’s topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

**TX Rate** – Transmission Rate.

**UDP** (**U**ser **D**atagram **P**rotocol) - A communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.

Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

**URL** (**U**niform **R**esource **L**ocator) - The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

**UTP** - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

**VLAN** (**V**irtual **LAN**) - A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

**Virtual Server** - Multiple servers that appear as one server, or one system image, to the operating system or for network administration.

**Wake-on-LAN** - Wake on LAN is a technology that allows a network professional to remotely power on a computer or to wake it up from *sleep mode*.

**WAN** - A communications network that covers a wide geographic area, such as a state or country.

**WEP** (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11 standard.

**WINIPCFG** - Configuration utility based on the Win32 API for querying, defining, and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

**Workgroup** - Two or more individuals that share files and databases.

**Upgrade** - To replace existing software or firmware with a newer version.

**Upload** - To send a file transmitted over a network. In a communications session, upload means transmit, and download means receive.

# Appendix B: The OSI Reference Model

Virtually all networks in use today are based in some fashion on the **Open Systems Interconnection** (OSI) standard. **OSI** was developed in 1984 by the International Organization for Standardization (ISO), a global federation representing approximately 130 countries.

The core of this standard is the **OSI Reference Model**, a set of seven layers that define the different stages that data must go through to travel from one device to another over a network. At each layer, certain things happen to the data that prepare it for the next layer.

The seven layers, which separate into **two sets**, are:

**Application Set**

**Layer 7: Application** - This is the layer that actually interacts with the operating system or application whenever the user chooses to transfer files, read messages or perform other network-related activities.

**Layer 6: Presentation** - Layer 6 takes the data provided by the Application layer and converts it into a standard format that the other layers can understand.

**Layer 5: Session** - Layer 5 establishes, maintains and ends communication with the receiving device.

**Transport Set**

**Layer 4: Transport** - This layer maintains **flow control** of data and provides for error checking and recovery of data between the devices. Flow control means that the Transport layer looks to see if data is coming from more than one application and integrates each application's data into a single stream for the physical network.

**Layer 3: Network** - The way that the data will be sent to the recipient device is determined in this layer. Logical protocols, routing, and addressing are handled here.

**Layer 2: Data** - In this layer, the appropriate physical protocol is assigned to the data. In addition, the type of network and the packet sequencing is defined.

**Layer 1: Physical** - This is the level of the actual hardware. It defines the physical characteristics of the network such as connections, voltage levels and timing.

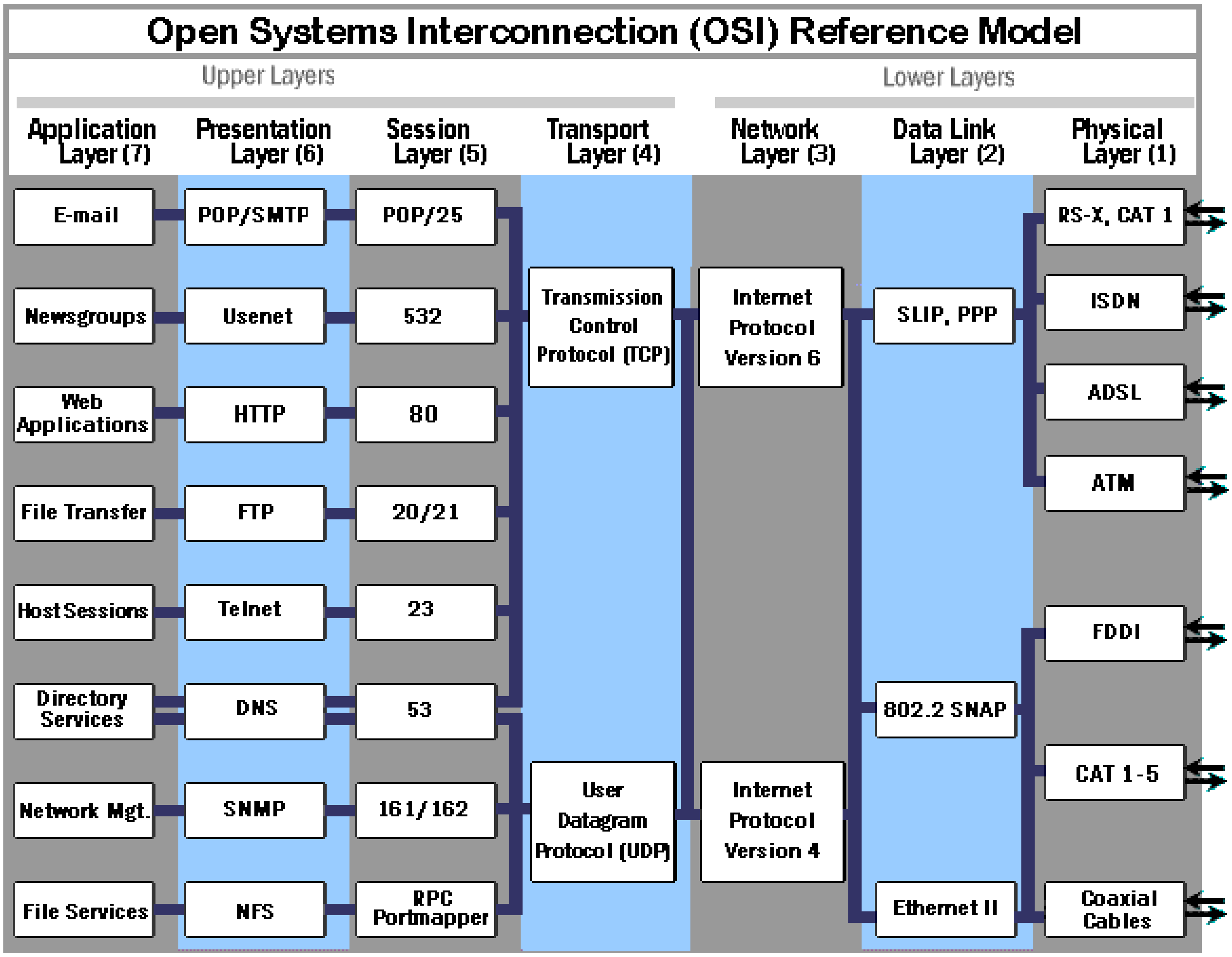
The OSI Reference Model is simply a guideline. Actual **protocol stacks** often combine one or more of the layers.

A protocol stack is a group of protocols that all work together to allow software or hardware to perform a function. For example, the **TCP/IP** (and UDP/IP) protocol stack uses four layers that map to the OSI model as follows:

**Layer 1: Network Interface** - This layer combines the Physical and Data layers and routes the data between devices on the same network. It also manages the exchange of data between the network and other devices.

**Layer 2: Internet** - This layer corresponds to the Network layer. The **Internet Protocol** (IP) uses the IP address, consisting of a network identifier and host identifier, to determine the address of the device with which it is communicating.

**Layer 3: Transport** - Corresponding to the OSI Transport layer, this is the part of the protocol stack where the **Transport Control Protocol** (TCP) and **User Datagram Protocol** (UDP) implemented by e-Control can be found. TCP works by asking another device on the network if it is willing to accept information from the local device.



**Layer 4: Application** - Layer 4 combines the Session, Presentation and Application layers of the OSI model. Protocols for specific functions such as email (**Simple Mail Transfer Protocol**, **SMTP**) and file transfer (**File Transfer Protocol**, **FTP**) reside at this level.

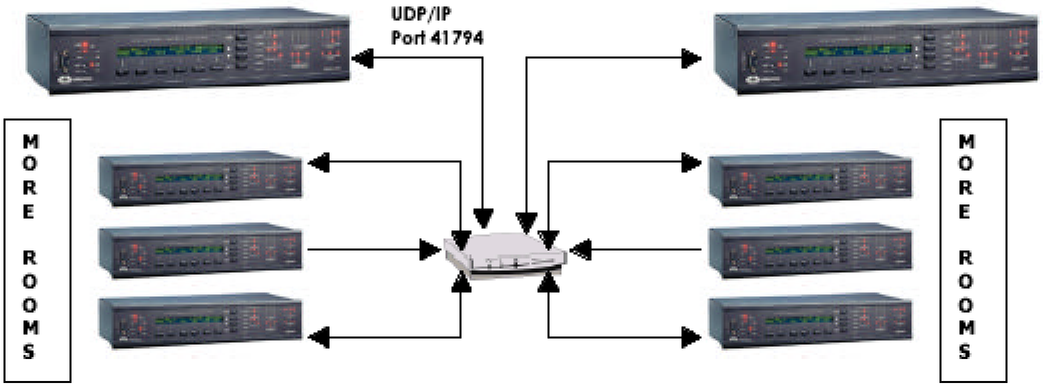
*OSI illustration copyrighted by and reused with permission of whatis.com (http://www.whatis.com) and TechTarget, Inc.*

# Appendix C: Control System Timing Data

### X-Series Control Systems

***Application:*** System to System Communications

***Overview:*** Multiple CNMSX processors can communicate and share data via LAN/WAN/Internet without the need of a PC. CNMSX communicates via the computer industry standard UDP/IP with built in error correction and retry so the data will pass across the network seamlessly and co-exist with all other applications.



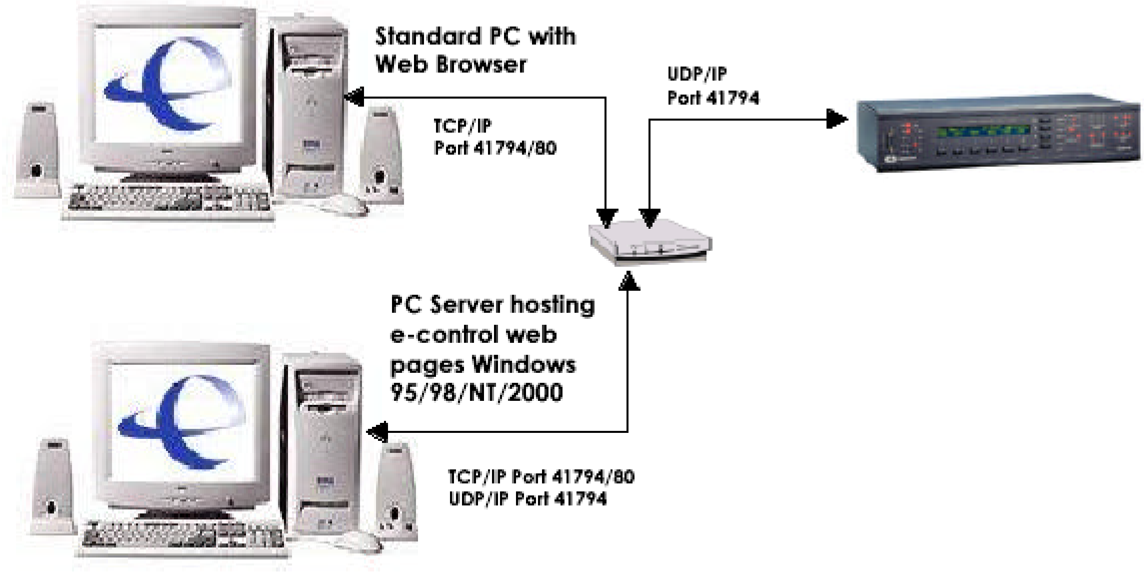
***PROTOCOLS & PORT NUMBERS:*** 10 BaseT Ethernet-Exchange Data using UDP Port 41794. ***Note:*** *CNMSX requires static IP address.*

***NETWORK ACTIVITY & RESPONSE TIME PREDICATIONS:***

| TASK | DESCRIPTION | PACKETS | BYTES SENT | BYTES RECEIVED | ELAPSED TIME |
|---|---|---|---|---|---|
| Digital signal assertion & release | Button Press | 2 packets sent and acknowledged | 120 | 120 | 14msec |
| Analog signal 10 step transmission | Bargraphs, Volume Control | 10 packets sent and acknowledged | 600 | 600 | 70msec |
| Serial string (256 bytes long) | Indirect text | Single larger packet sent and acknowledged | 300 | 60 | 7msec |

***Application:*** Web pages hosted on a PC/Server using the Crestron CNX Gateway connected to one or more control systems

***Overview:*** With Crestron's VTPro-e or Crestron's Software Development Kit (SDK), you can design web pages for a remote GUI control of your AV equipment. With Crestron e-control all you need is a host computer on the corporate LAN/WAN, and you have access to remote room control that is as easy to operate as surfing the web.


Standard PC with Web Browser
TCP/IP Port 41794/80
UDP/IP Port 41794
PC Server hosting e-control web pages Windows 95/98/NT/2000
TCP/IP Port 41794/80
UDP/IP Port 41794

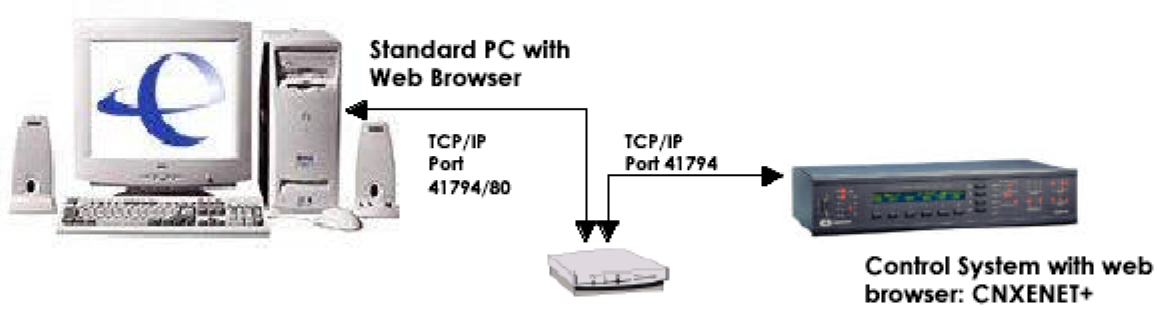
***PROTOCOLS & PORT NUMBERS:*** 10 BaseT Ethernet-Exchange Data using TCP Port 41794 and Port 80, and UDP Port 41794. ***Note:*** *CNMSX requires static IP address.*

***NETWORK ACTIVITY & RESPONSE TIME PREDICATIONS:***

| TASK | DESCRIPTION | PACKETS | BYTES SENT | BYTES RECEIVED | ELAPSED TIME |
|---|---|---|---|---|---|
| Digital signal assertion & release | Button Press | 4 packets sent and acknowledged | 240 | 240 | 15msec |
| Analog signal 10 step transmission | Bargraphs, Volume Control | 20 packets sent and acknowledged | 1200 | 1200 | 74msec |
| Serial string (256 bytes long) | Indirect text | 2 larger packet sent and acknowledged | 600 | 120 | 8msec |

***Application:*** Web pages hosted internal to the control system on a CNXENET+ card

***Overview:*** Web pages can be hosted directly on the CNXENET+ card without the need for an external PC or additional software.



***PROTOCOLS & PORT NUMBERS:*** 10 BaseT Ethernet-Exchange Data using TCP/IP Port 41794. ***Note:*** *CNMSX requires static IP address.*

***NETWORK ACTIVITY & RESPONSE TIME PREDICATIONS:***

| **TASK** | **DESCRIPTION** | **PACKETS** | **BYTES SENT** | **BYTES RECEIVED** | **ELAPSED TIME** |
|---|---|---|---|---|---|
| **Digital signal assertion & release** | **Button Press** | **2 packets sent and acknowledged** | **120** | **120** | **14msec** |
| **Analog signal 10 step transmission** | **Bargraphs, Volume Control** | **10 packets sent and acknowledged** | **600** | **600** | **70msec** |
| **Serial string (256 bytes long)** | **Indirect text** | **Single larger packet sent and acknowledged** | **300** | **60** | **7msec** |

***Diagnostics/Console:*** Crestron offers complete remote diagnostics for X Generation Control Systems via TCP/IP Port 41795.

***Conclusion:*** In a typical control application, the CNMSX will send data at a peak rate of 150 packets per second. The typical control packet is 60 bytes long. At this rate, the peak network utilization is only 90kbit/sec. If a large amount of string data is transmitted, then the peak rate would be higher. For example, if there are 150 messages of 256 byte strings sent in a second, then the peak network rate would be 450kbit/sec. This is a small fraction of even a 10BaseT network's bandwidth. The sustained traffic rate is much lower. For further information, please contact Crestron Technical Sales at 1.800.237.2041.

# Appendix D: Web Server Console Commands

## PRO2 Help options for Ethernet

```
PRO2>help ether
ADDMaster        Add a “master” entry to IP table.
ADDPortmap       Add a port map to the NAT table.
CIPPORT          Set port number for CIP.
CTPPORT          Set port number for CTP (console).
DEFRouter        Set default router.
ESTatus          Display the status of the Ethernet.
ETHERNET         Enable/disable Ethernet.
ETHERTEST        Start Ethernet test.
HOSTname         Set the host name for DNS environment.
IPAddress        Set IP address.
IPMask           Set IP subnet mask.
IPTable          Display IP table.
KILLSOCKET       Cancel an active TCP console socket.
NATENAble        Enable/disable Network Address Translator (NAT).
NATREMote        Enable/disable NAT Remote Config.
PING             Ping remote node.
REMMaster        Remove an entry from IP table.
REMPortmap       Remove a port map from the NAT table.
SHOWPORTMAP      Display the current portmaps for the NAT.
WEBSERVer        Enable/disable Webserver.
WEBINIT          Initialize Webserver default file.
WEBPORT          Set port number for Webserver.
WHO              Generate a report of the Ethernet consoles.
```

## X-Series/CNXENET+ Help options for Ethernet

*X-Series processors with a CNXENET+ card must have 51263 ops to control the web port interface.

```
Version 5.12.63-x   11/14/2001

__?                       Dir
_MAC_Adr                  Free
IP_Adr                    Del
IP_Mask                   Initialize
IP_MTU                    Xputfile
Def_router                Type
Password                  Test1
Ver
Info                      To change web port:
Restart                   [ESC]x’web[SPACE]”newport #”[ENTER]
then
Web                       reboot
LimitWeb
```

## SSL Console Commands

For security, all SSL commands are only allowed from a serial connection to the console.

*SSL [OFF | SELF | CA]*

*'OFF' turns off SSL,*

*'SELF' sets SSL to use 'self-signed' certificates,*

*'CA' sets SSL to use 'CA' issued certificates,*

*No parameter - displays current setting*

This command turns the SSL mode on or off. For example, when SSL is on, typing "SSL" displays the current settings as follows: >*SSL: ON,CA.* This indicates that SSL is turned ON and set to read the CA generated certificate.

When SSL is off, typing SSL displays the current settings as follows:

*SSL: OFF,CA*

This is interpreted as "SSL is OFF and the previous setting ***was*** set to read CA generated certificate".

*CREATECSR CN:SN:LN:ON:OUN:SN:EA:*

*CN = 2 letter country code*

*SN = Full state or province name*

*LN = Locality or city name*

*ON = Organization or company name*

*OUN= Organizational Unit name or division*

*SN = site name or domain name*

*EA = Email address*

This command creates a CSR. For example, when CREATECSR is run without any parameters, a default CSR will be created.

*XLOADCERTFILE size date time name*

*size - size of the file in bytes*

*date - date of the file (MM-DD-YY)*

*time - time of the file (HH:MM:SS)*

*name - name of the file*

This command loads a certificate file onto the processor. The command works exactly like the XPUTFILE command, only the "name" parameter should be set to "srv_cert.der". The "size", "date" and "time" parameters should be determined from the certificate file stored in the host system after obtaining it from a CA. The stored certificate file in the host is the format *.CER, which is an ASCII file. The command will convert the file to "\\sys\srv_cert.der".

# Appendix E: FAQ for IT/MIS professionals

**What is a Crestron Control System?**
A Crestron Control System is a programmable device that allows control of external devices (typically of Audio/Visual nature), by means of a serial connection, relays, infrared, and IP. Additional capabilities include MIDI interface, digital or analog inputs. Crestron Control Systems use several different input devices for user interaction; these include touchpanels and button panels.

**Why does it need to be connected to our corporate LAN?**
The Crestron Control system uses Ethernet for:

Intersystem communication – From one Crestron system to another.

Remote control – The program running on the control system can allow for remote users to interface with the program over IP. These devices can be Wintel machines, pocket PCs, or Web tablets.

Remote monitoring – Crestron programs can be run on a PC to monitor the status of all Crestron control processors on the network.

Web interface – The Crestron control processor comes with a built-in Web server that is used for serving up Web pages that communicate with the program. These pages contain HTML as well as Java, or Active X objects.

**Ethernet Adapter**
The Ethernet adapter uses a standard RJ45 connector, utilizing pins 1, 2, 3, and 6. It supports 10Mbs, 100Mbs Half Duplex, and 100Mbs Full Duplex. It also has an auto negotiation setting, which will "sync" up with the router/hub/switch it is connected to.

**What is the dual Ethernet port for?**
The dual Ethernet port enables a private network that is not connected to the production network. The devices on the private network will be addressable from the production network using NAT. Any broadcasts on the private network will not be seen on the production network.

**What are typical traffic patterns for Crestron Systems?**
Crestron uses mostly TCP connections (Web server, and Telnet), but also can use UDP for intersystem communications. Only IP traffic is used, no NETBIOS, NETBEUI, or IPX/SPX.

Broadcasts: If the unit is set up for DHCP, it will send out the necessary broadcasts in order to obtain a valid IP address. Also, the unit will occasionally send out an ARP request. All other communications are unicast.

The amount of traffic generated by, or routed to the Crestron system all depends on the customized program that has been uploaded, and the amount of connections that are made.

One of the features of the Crestron Control Processor is that it has a built-in Web server. This Web server is used for serving up pages that communicate directly with the processor. These pages contain HTML, as well as Java or ActiveX objects.

**Static or DHCP?**

Because of the many uses of the Crestron Control System (Server, IP to RS232 Gateway, NAT Router), and the fact that many diverse clients connect to the processor over IP, it may be desired to configure the systems for static IP addresses (as would a web server, or a router).

Crestron Control Systems also provide DHCP support with the following configurations:

*DHCP + Dynamic DNS (Windows 2000)*

The DHCP Scope has to include the following options:
- 003 – Router
- 006 – DNS Servers
- 015 – Domain Name

The DHCP Scope should have the following settings enabled:
- Always dynamically update all nodes
- Enable updating of nodes that don't support dynamic DNS

The DNS Server should have the following setting enabled:
- Handle Dynamic Updates

*DHCP + WINS + DNS (Windows 2000 or Windows NT 4)*

The DHCP Scope has to include the following options:
- 003 – Router
- 006 – DNS Servers
- 015 – Domain Name
- 044 – WINS/NBNS Servers
- 040 – WINS/NBT Node Type (Set value to '0x2')

The DNS Server should have the following setting enabled:
- Enable WINS Resolution (Windows NT 4.0)
- Enable WINS Forward Lookup (Windows 2000)

# Software License Agreement

This License Agreement ("Agreement") is a legal contract between you (either an individual or a single business entity) and Crestron Electronics, Inc. ("Crestron") for software referenced in this guide, which includes computer software and, as applicable, associated media, printed materials, and "online" or electronic documentation (the "Software").

BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU REPRESENT THAT YOU ARE AN AUTHORIZED DEALER OF CRESTRON PRODUCTS OR A CRESTRON AUTHORIZED INDEPENDENT PROGRAMMER AND YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE.

IF YOU HAVE PAID A FEE FOR THIS LICENSE AND DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, CRESTRON WILL REFUND THE FEE TO YOU PROVIDED YOU (1) CLICK THE DO NOT ACCEPT BUTTON, (2) DO NOT INSTALL THE SOFTWARE AND (3) RETURN ALL SOFTWARE, MEDIA AND OTHER DOCUMENTATION AND MATERIALS PROVIDED WITH THE SOFTWARE TO CRESTRON AT: CRESTRON ELECTRONICS, INC., 15 VOLVO DRIVE, ROCKLEIGH, NEW JERSEY 07647, WITHIN 30 DAYS OF PAYMENT.

LICENSE TERMS

Crestron hereby grants You and You accept a nonexclusive, nontransferable license to use the Software (a) in machine readable object code together with the related explanatory written materials provided by Creston (b) on a central processing unit ("CPU") owned or leased or otherwise controlled exclusively by You, and (c) only as authorized in this Agreement and the related explanatory files and written materials provided by Crestron.

If this software requires payment for a license, you may make one backup copy of the Software, provided your backup copy is not installed or used on any CPU. You may not transfer the rights of this Agreement to a backup copy unless the installed copy of the Software is destroyed or otherwise inoperable and You transfer all rights in the Software.

You may not transfer the license granted pursuant to this Agreement or assign this Agreement without the express written consent of Crestron.

If this software requires payment for a license, the total number of CPU's on which all versions of the Software are installed may not exceed one per license fee (1) and no concurrent, server or network use of the Software (including any permitted back-up copies) is permitted, including but not limited to using the Software (a) either directly or through commands, data or instructions from or to another computer (b) for local, campus or wide area network, internet or web hosting services; or (c) pursuant to any rental, sharing or "service bureau" arrangement.

The Software is designed as a software development and customization tool. As such Crestron cannot and does not guarantee any results of use of the Software or that the Software will operate error free and You acknowledge that any development that You perform using the Software or Host Application is done entirely at Your own risk.

The Software is licensed and not sold. Crestron retains ownership of the Software and all copies of the Software and reserves all rights not expressly granted in writing.

OTHER LIMITATIONS

You must be an Authorized Dealer of Crestron products or a Crestron Authorized Independent Programmer to install or use the Software. If Your status as a Crestron Authorized Dealer or Crestron Authorized Independent Programmer is terminated, Your license is also terminated.

You may not rent, lease, lend, sublicense, distribute or otherwise transfer or assign any interest in or to the Software.

You may not reverse engineer, decompile, or disassemble the Software.

You agree that the Software will not be shipped, transferred or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations ("Export Laws"). By downloading or installing the Software You (a) are certifying that You are not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria or any country to which the United States embargoes goods (b) are certifying that You are not otherwise prohibited from receiving the Software and (c) You agree to comply with the Export Laws.

If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms. This Agreement may only be modified by a writing signed by an authorized officer of Crestron. Updates may be licensed to You by Crestron with additional or different terms. This is the entire agreement between Crestron and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software. The failure of either party to enforce any right or take any action in the event of a breach hereunder shall constitute a waiver unless expressly acknowledged and set forth in writing by the party alleged to have provided such waiver.

If You are a business or organization, You agree that upon request from Crestron or its authorized agent, You will within thirty (30) days fully document and certify that use of any and all Software at the time of the request is in conformity with Your valid licenses from Crestron of its authorized agent.

Without prejudice to any other rights, Crestron may terminate this Agreement immediately upon notice if you fail to comply with the terms and conditions of this Agreement. In such event, you must destroy all copies of the Software and all of its component parts.

PROPRIETARY RIGHTS

*Copyright*. All title and copyrights in and to the Software (including, without limitation, any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software), the accompanying media and printed materials, and any copies of the Software are owned by Crestron or its suppliers. The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software like any other copyrighted material, subject to the provisions of this Agreement.

*Submissions.* Should you decide to transmit to Crestron's website by any means or by any media any materials or other information (including, without limitation, ideas, concepts or techniques for new or improved services and products), whether as information, feedback, data, questions, comments, suggestions or the like, you agree such submissions are unrestricted and shall be deemed non-confidential and you automatically grant Crestron and its assigns a non-exclusive, royalty-tree, worldwide, perpetual, irrevocable license, with the right to sublicense, to use, copy, transmit, distribute, create derivative works of, display and perform the same.

*Trademarks.* CRESTRON and the Swirl Logo are registered trademarks of Crestron Electronics, Inc. You shall not remove or conceal any trademark or proprietary notice of Crestron from the Software including any back-up copy.

GOVERNING LAW

This Agreement shall be governed by the laws of the State of New Jersey, without regard to conflicts of laws principles. Any disputes between the parties to the Agreement shall be brought in the state courts in Bergen County, New Jersey or the federal courts located in the District of New Jersey. The United Nations Convention on Contracts for the International Sale of Goods, shall not apply to this Agreement.

CRESTRON LIMITED WARRANTY

CRESTRON warrants that: (a) the Software will perform substantially in accordance with the published specifications for a period of ninety (90) days from the date of receipt, and (b) that any hardware accompanying the Software will be subject to its own limited warranty as stated in its accompanying written material. Crestron shall, at its option, repair or replace or refund the license fee for any Software found defective by Crestron if notified by you within the warranty period. The foregoing remedy shall be your exclusive remedy for any claim or loss arising from the Software.

CRESTRON shall not be liable to honor warranty terms if the product has been used in any application other than that for which it was intended, or if it as been subjected to misuse, accidental damage, modification, or improper installation procedures. Furthermore, this warranty does not cover any product that has had the serial number or license code altered, defaced, improperly obtained, or removed.

Notwithstanding any agreement to maintain or correct errors or defects Crestron, shall have no obligation to service or correct any error or defect that is not reproducible by Crestron or is deemed in Crestron's reasonable discretion to have resulted from (1) accident; unusual stress; neglect; misuse; failure of electric power, operation of the Software with other media not meeting or not maintained in accordance with the manufacturer's specifications; or causes other than ordinary use; (2) improper installation by anyone other than Crestron or its authorized agents of the Software that deviates from any operating procedures established by Crestron in the material and files provided to You by Crestron or its authorized agent; (3) use of the Software on unauthorized hardware; or (4) modification of, alteration of, or additions to the Software undertaken by persons other than Crestron or Crestron's authorized agents.

ANY LIABILITY OF CRESTRON FOR A DEFECTIVE COPY OF THE SOFTWARE WILL BE LIMITED EXCLUSIVELY TO REPAIR OR REPLACEMENT OF YOUR COPY OF THE SOFTWARE WITH ANOTHER COPY OR REFUND OF THE INITIAL LICENSE FEE CRESTRON RECEIVED FROM YOU FOR THE DEFECTIVE COPY OF THE PRODUCT. THIS WARRANTY SHALL BE THE SOLE AND EXCLUSIVE REMEDY TO YOU. IN NO EVENT SHALL CRESTRON BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES OF ANY KIND (PROPERTY OR ECONOMIC DAMAGES INCLUSIVE), EVEN IF A CRESTRON REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR OF ANY CLAIM BY ANY THIRD PARTY. CRESTRON MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO TITLE OR INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY OTHER WARRANTIES, NOR AUTHORIZES ANY OTHER PARTY TO OFFER ANY WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY FOR THIS PRODUCT. THIS WARRANTY STATEMENT SUPERSEDES ALL PREVIOUS WARRANTIES.

# Return and Warranty Policies

## Merchandise Returns / Repair Service

1. No merchandise may be returned for credit, exchange, or service without prior authorization from CRESTRON. To obtain warranty service for CRESTRON products, contact the factory and request an RMA (Return Merchandise Authorization) number. Enclose a note specifying the nature of the problem, name and phone number of contact person, RMA number, and return address.
2. Products may be returned for credit, exchange, or service with a CRESTRON Return Merchandise Authorization (RMA) number. Authorized returns must be shipped freight prepaid to CRESTRON, Cresskill, N.J., or its authorized subsidiaries, with RMA number clearly marked on the outside of all cartons. Shipments arriving freight collect or without an RMA number shall be subject to refusal. CRESTRON reserves the right in its sole and absolute discretion to charge a 15% restocking fee, plus shipping costs, on any products returned with an RMA.
3. Return freight charges following repair of items under warranty shall be paid by CRESTRON, shipping by standard ground carrier. In the event repairs are found to be non-warranty, return freight costs shall be paid by the purchaser.

### CRESTRON Limited Warranty

CRESTRON ELECTRONICS, Inc. warrants its products to be free from manufacturing defects in materials and workmanship under normal use for a period of three (3) years from the date of purchase from CRESTRON, with the following exceptions: disk drives and any other moving or rotating mechanical parts, pan/tilt heads and power supplies are covered for a period of one (1) year; touchscreen display and overlay components are covered for 90 days; batteries and incandescent lamps are not covered.

This warranty extends to products purchased directly from CRESTRON or an authorized CRESTRON dealer. Purchasers should inquire of the dealer regarding the nature and extent of the dealer's warranty, if any.

CRESTRON shall not be liable to honor the terms of this warranty if the product has been used in any application other than that for which it was intended, or if it has been subjected to misuse, accidental damage, modification, or improper installation procedures. Furthermore, this warranty does not cover any product that has had the serial number altered, defaced, or removed.

This warranty shall be the sole and exclusive remedy to the original purchaser. In no event shall CRESTRON be liable for incidental or consequential damages of any kind (property or economic damages inclusive) arising from the sale or use of this equipment. CRESTRON is not liable for any claim made by a third party or made by the purchaser for a third party.

CRESTRON shall, at its option, repair or replace any product found defective, without charge for parts or labor. Repaired or replaced equipment and parts supplied under this warranty shall be covered only by the unexpired portion of the warranty.

Except as expressly set forth in this warranty, CRESTRON makes no other warranties, expressed or implied, nor authorizes any other party to offer any other party to offer any warranty, including any implied warranties of merchantability or fitness for a particular purpose. Any implied warranties that may be imposed by law are limited to the terms of this limited warranty. This warranty statement supercedes all previous warranties.

**Trademark Information**
*All brand names, product names, and trademarks are the sole property of their respective owners. Windows is a registered trademark of Microsoft Corporation. Windows95/98/Me/XP and WindowsNT/2000 are trademarks of Microsoft Corporation.*

This page intentionally left blank.

This page intentionally left blank.

**Crestron Electronics, Inc.**
15 Volvo Drive   Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

**Reference Guide – DOC. 6052**
**7.03**