Best Practices

IP Guidelines for the IT Professional

Crestron Electronics, Inc.

Original Instructions
The U.S. English version of this document is the original instructions.
All other languages are a translation of the original instructions.

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/opensource.

Crestron, the Crestron logo, 3-Series, 4-Series, .AV Framework, CaptureLiveHD, Crestron Connected, Crestron Fusion, Crestron Mobile Pro, Crestron Toolbox, DigitalMedia, DM, Fusion RV, and Smart Graphics are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Flash is either a trademark or registered trademark of Adobe Systems Incorporated in the United States and/or other countries. iPad is either a trademark or registered trademark of Apple, Inc. in the United States and/or other countries. Blu-ray is either a trademark or registered trademark of the Blu-ray Disc Association (BDA) in the United States and/or other countries. HDMI is either a trademark or registered trademark of HDMI Licensing LLC in the United States and/or other countries. Active Directory and ActiveX are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Java is either a trademark or registered trademark of Oracle Corporation. in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

Contents

Introduction

This document outlines the requirements, best practices, and preferred methods of implementing Crestron® devices on enterprise-level networks. It focuses on the concerns of the IT professional.

> **NOTE:** Contact Crestron True Blue support via phone, email, or chat as described at www.crestron.com/Support for any concerns about deploying Crestron devices on a network.

What Is a Control System?

A control system is an appliance-grade, network-based component designed to control different devices and link them together over an IP network. A control system issues commands and gathers data from other devices based on user-driven and automated events. Typically driving AV systems, a control system turns on the display and sets the correct input via a touch screen, remote control, or keypad. Control systems can also interface with lighting and HVAC systems so that, for example, when a PC is selected from a button panel or touch screen, the lights dim to an appropriate level for viewing computer images. Crestron control systems can be custom programmed or configured. A single button press or collection of data can trigger a number of events.

Why Is a Control System on My Network?

Traditionally, control systems interfaced with devices via IR, RS-232, closed contacts, and variable voltage. The progression in recent years has moved to IP-based communication. Many devices have implemented IP protocols for control, monitoring, and management because IP is more common and cost effective to integrate.

Crestron offers advanced IP devices that can be controlled, maintained, and monitored from anywhere with an Internet connection. This greatly enhances the ability to update and troubleshoot systems without the need to be physically on site.

Plan a Network

Before deploying a Crestron system on a network, it is important to consider the guidelines presented in this section. While there are many ways to configure an enterprise network, these practices have been found to be the most efficient and successful for Crestron devices.

Isolate the Network

Crestron devices should exist on a network separate from other device traffic. Other network activity can impact the response time of Crestron devices and disrupt the user experience.

Crestron users expect instant control and feedback. To ensure constant connection and accurate feedback, proprietary Crestron control communication uses a heartbeat packet. Loss of round-trip heartbeat packets indicates unreliable connections. Crestron control systems have strict response time and connectivity requirements to ensure user confidence and, as such, are very latency sensitive. Therefore, Crestron recommends setting up all Crestron devices on a dedicated (Crestron-only) VLAN so that unnecessary traffic does not interfere with the time-sensitive packets between Crestron devices.

Deploying Crestron devices on a dedicated VLAN provides network access control in addition to the username and password authentication that is available on Crestron control systems.

VLAN Configuration

Whenever possible, all Crestron devices should be separate on their own VLAN. This allows for smoother operation of the control network and helps manage infrastructure, resulting in a better user experience.

The following steps should be taken to ensure that Crestron devices can be managed effectively:

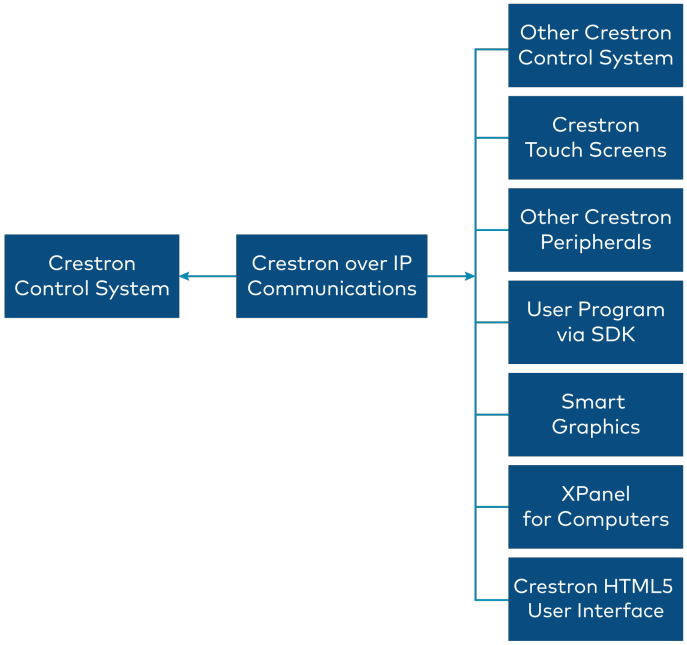
- If Crestron devices reside on multiple VLANs, static routes should be set up between VLANs on a router.
- Dynamic Host Configuration Protocol (DHCP) requests should be forwarded to the appropriate VLAN with a DHCP server.
- For proper operation, Crestron ports should not be blocked. For detailed information regarding the required port numbers for a 4-Series control system, refer to the 4-Series Control Systems Reference Guide.
- Some devices allow streaming media content from the internet. These devices should be allowed to connect to the internet if streaming is desired.
- A 16-port switch such as the CEN-SWPOE-16 supports VLANs, which is useful when designing a Crestron network.

Listen Ports

A Crestron control system listens to the following set of ports. Not all ports are turned on by default. For detailed information regarding the required port numbers for a 4-Series control system, refer to the 4-Series Control Systems Reference Guide.

Port	Protocol	Service	Notes
22	TCP	SSH/SFTP	
80	TCP	Web access	For user program interface and setup pages Required for XPanel with Smart Graphics® using a web interface
161	UDP	SNMP	
443	TCP	Web access	Active with SSL enabled
41794	TCP/UDP	Crestron over IP	Proprietary Crestron control communications
41796	TCP	Crestron over IP	Active with SSL enabled
49200	TCP	Secure WebSocket server	For Crestron HTML5 User Interface

Crestron over IP Communications



Multiple listeners can be added to the Crestron control system via the user program. Crestron recommends performing a security scan on the control system without a program and then performing the scan again with a program. This will help identify whether any security breaches are created by loading the program.

Connect Ports

Using external devices and services, a Crestron control system can connect to the following sets of ports. Not all ports are turned on by default. For detailed information regarding the required port numbers for a 4-Series control system, refer to the 4-Series Control Systems Reference Guide.

Port	Protocol	Service	Notes
42	TCP/UDP	WINS access	
53	UDP	DNS access	
67/68	UDP	DHCP configuration	
80	TCP	HTTP	
161/162	UDP	SNMP	
443	TCP	HTTPS	
41794	TCP/UDP	Crestron over IP	Proprietary Crestron control communications
41796	TCP	Crestron over IP	Active with SSL enabled

IP Addressing

In most installations, Crestron recommends configuring devices with static IP addresses. Especially in large corporate or university environments, using static or reserved DHCP aids in managing devices and avoids potential DNS issues. However, DHCP should be used when devices are connected to a Crestron control subnet. See Crestron Control Subnet on page 6 for more information.

IPv6

All Crestron Ethernet devices can exist on an IPv6 network. Certain Crestron Ethernet devices support IPv6 addressing, which can be turned on using the device's web configuration interface or console commands via Crestron Toolbox™ software. The device's web configuration interface can be accessed over IPv6 by entering its IPv6 address into a web browser (**https://[ipv6address]**).

The following table lists the Crestron Ethernet device categories that currently support IPv6 addressing with the minimum firmware version that adds this support.

Device Category	Minimum Firmware Version
4-Series™ Control Systems	2.8001.*x*
DM NVX® A/V Encoders and Decoders	7.1.*x*
TS/TSS/TSW-70 Series Touch Screens	2.003.*x*

NOTE: Refer to the firmware release notes for the specific device models that support this functionality and for any device-specific IPv6 limitations that may exist.

The following software and services are not supported by Crestron Ethernet devices over IPv6 addressing:

- BACnet
- SNMP
- Crestron Fusion® software
- Crestron modules and IP drivers
- XPanel (must use a host name that can resolve to an IPv6 address)
- .AV Framework™ software

Hostnames

Crestron recommends configuring DNS and DHCP servers to allow hostnames to resolve via option 81 or option 12.

Crestron Control Subnet

The Crestron Control Subnet is a Gigabit Ethernet network dedicated to Crestron devices for fast system updating and troubleshooting. This feature is available on select 4-Series control systems (AV4, CP4N, and PRO4). The Control Subnet ports provide seamless connectivity to the network, requiring just one IP address for the entire Crestron system. This enables better performance while maintaining the integrity of the IT network.

Crestron installers can access devices within the Control Subnet via the host name using Crestron Toolbox™ software. This makes it easier to upload touch screen projects, to upload firmware, and to access other functions.

Configuration

All Crestron Ethernet devices should be connected to the Control Subnet except for the devices that provide streams to the LAN, such as security cameras, CaptureLiveHD® system devices, and network video streamers. These devices should be connected to the LAN and not to the Control Subnet.

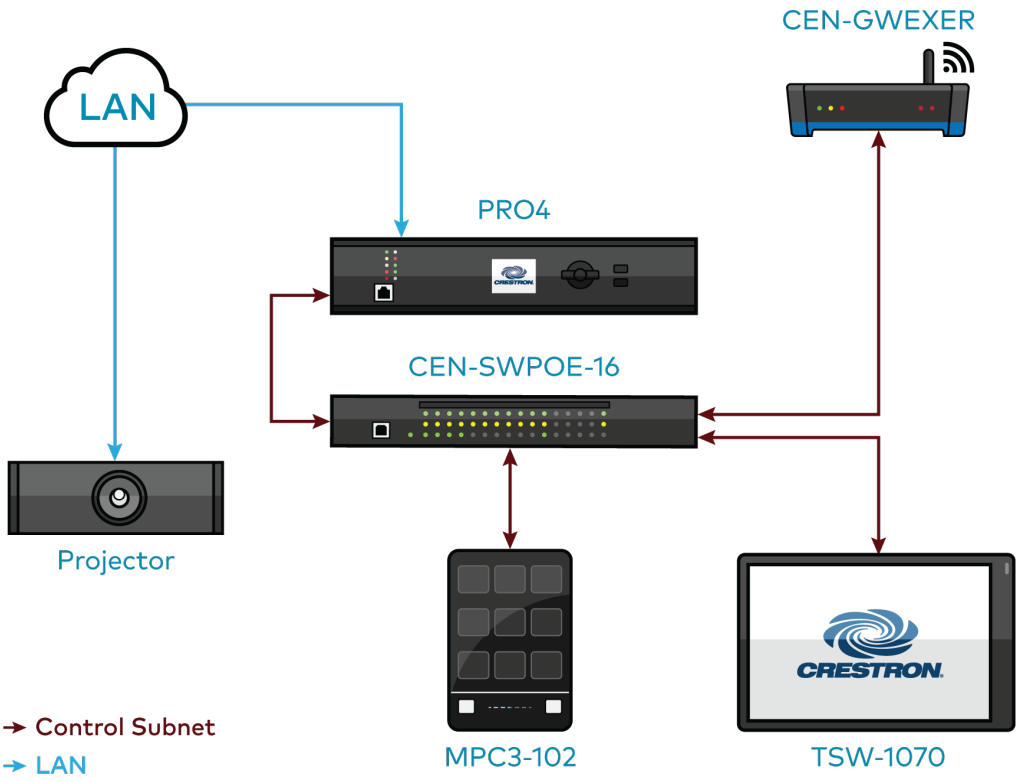
There is no enforced limit to the number of devices that are supported on the Control Subnet. While the subnet mask provides an upper limit, Ethernet best practices should be followed to determine the appropriate number of devices for the network.

Crestron devices should be set to DHCP mode, which allows the Control Subnet DHCP server to assign addresses. Unlike on a public network, Crestron requires all devices on the Control Subnet to be in DHCP mode. Reserved DHCP leases can be set up on the control subnet. The control subnet cannot run in static mode. When on the control subnet, a DigitalMedia™ system should be in Private network Mode (PNM).

NOTES:

- Some DM® streaming cards support two network connections. These streaming cards can reside in a DM chassis on the Control Subnet, but their external network connections should be to the corporate LAN.
- When another DHCP server is detected, the control subnet port is shut down. Therefore, do not connect the Control Subnet port to the corporate LAN.
- Crestron does not recommend connecting third-party devices to the Control Subnet. Only Crestron and Crestron Connected® devices should be connected to the Control Subnet.
- Two Control Subnet ports may not be connected together on the same network.

Control Subnet Example



Listen Ports

Listen ports are used for configuration changes for Crestron devices on the Control Subnet. Listen ports open and close dynamically. On the Control Subnet, the number of listen posts on the LAN changes. There are 400 open listen ports. Crestron utilizes listen ports ranging from 64000 to 64399.

IP Addressing

The following IP addressing guidelines should be followed for Crestron devices.

Automatic Mode (Default)

In order to eliminate routing conflicts between the Control Subnet and the LAN, the Control Subnet IP address is automatically set based on the LAN-side Ethernet configuration. See the table below for information on Control Subnet IP addressing in automatic mode.

LAN	Control Subnet
Class A	Class B (172.22.0.0/16)
Class B	Class A (10.0.0.0/8)
Class C	Class B (172.22.0.0/16)

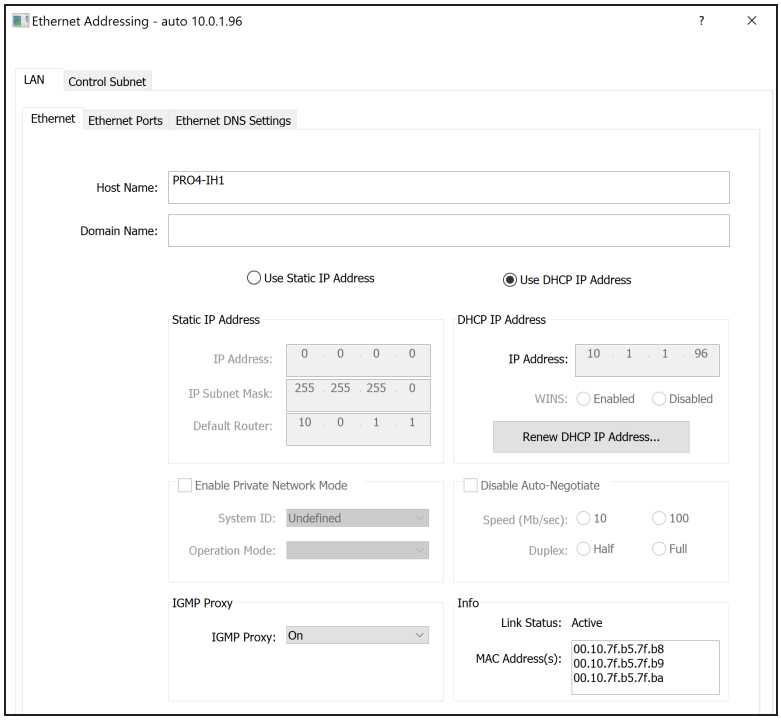
Manual Mode

There is usually no need to change the automatic settings. If necessary, the user can set the routing prefix for the Control Subnet manually. This should only be done if the LAN contains a network that conflicts with the Control Subnet.

> **NOTE:** If the routing prefix is set on the Control Subnet, any reserved leases are erased and the control system no longer checks for routing conflicts between the LAN and the Control Subnet. It is important that the user is familiar with how manual mode operates before proceeding.

To set the routing prefix for the Control Subnet manually:

1. From the EasyConfig tool within Crestron Toolbox, select **Ethernet Addressing**. The **Ethernet Addressing** window opens.



2. Select the **Control Subnet** tab.
3. Select **Manual** for the **Control Subnet**.
4. Enter the prefix for **Routing** in Classless Inter-Domain Routing (CIDR) notation, and select the bit length of the prefix after the **/**.

> **NOTE:** Only bit lengths from /8 to /24 are accepted. An example of a valid routing prefix is 172.22.0.0/16.

Hostnames

Crestron recommends changing host names to meaningful names. The Control Subnet allows port forwarding based on the host name of the device.

Security

The following security information is centered around 4-Series™ control systems. For more information, refer to the 4-Series™ Control Systems Security Reference Guide.

For more information on how to deploy a Crestron system in a secure environment, refer to https://security.crestron.com.

Security Setup

When setting up security on a 4-Series control system:

- An administrator account must be created upon initial connection to the control system to guarantee that only authorized personnel can make changes to the configuration of Crestron equipment. Authentication cannot be turned off on 4-Series control systems.
- Enable SSL/TLS to ensure that passwords are not sent as cleartext over the network.
- Have a Crestron programmer add passwords and passcodes to the sections of the user program that are related to the configuration of third-party devices.

Firewall Setup and Communication Across Multiple VLANs

Crestron systems can be controlled remotely. For example, an iPad® device running the Crestron Go App on a cellular network can send commands to the control system to adjust lights. This example would require the following ports in order to have access to the outside network:

Port	Protocol	Service	Notes
80	TCP	Web server	Web pages can also be hosted via IIS or other corporate web server
443	TCP	Secure web server	Use for secure SSL access
41794	TCP	Crestron over IP	Proprietary Crestron control communications
41796	TCP	Secure Crestron over IP	Proprietary Crestron control communications when SSL is enabled
49200	TCP	Secure Crestron over IP (for Crestron HTML5 User Interface)	Proprietary Crestron control communications over WebSocket when SSL is enabled

DigitalMedia Network Considerations

Most Crestron DigitalMedia™ devices are Ethernet devices. Ethernet traffic due to DigitalMedia devices is relatively low. The custom control system program that ties the DM system together dictates how much bandwidth is needed.

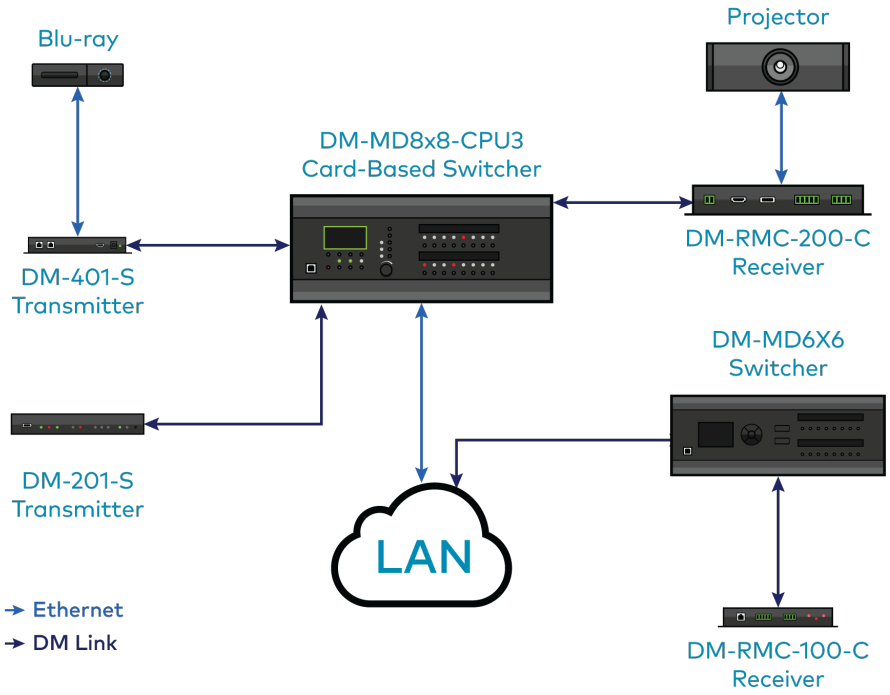
> **DigitalMedia Certified Designers and Engineers**
>
> Every Crestron DM® system should be designed by a DigitalMedia Certified Designer - 4K (DMC-D-4K) and commissioned by a DigitalMedia Certified Engineer - 4K (DMC-E-4K).
>
> Only Crestron certified engineers ensure that a system is properly installed and configured to Crestron standards. The information in this guide is intended to explain basic DM IP addressing guidelines. See the Crestron website for more information on DMC Training for 4K.

Each DM link (connection between two DM devices) carries Ethernet embedded inside. Therefore, no additional wiring is needed to provide network connectivity for third-party Ethernet products installed at the endpoints. Interconnected DM devices need only a single point (typically the main switcher) to be connected to the LAN in order to provide Ethernet to all devices in the system. To facilitate this, Crestron DM devices have integrated, managed Ethernet switches and an exposed Ethernet port.

> **NOTE:** A DM endpoint is any DM transmitter or receiver.

In the scenario below, Ethernet connectivity is provided to all DM devices and third-party devices from the single LAN connection at the DM-MD8X8(-CPU3). This eliminates the need to run extra wiring to each location to provide Ethernet connectivity.

DigitalMedia Ethernet Connectivity



The main Ethernet uplink to a DM system occurs at the DigitalMedia switcher.

The following switchers have 100BASE-TX/1000BASE-T autonegotiating uplink ports: DM-MD6X4, DM-MD6X6, DM-MD8X8(-CPU3), DM-MD16X16(-CPU3), DM-MD32X32(-CPU3), and all DMPS3 models.

The DM-MD6X1 switcher has 100BASE-TX autonegotiating uplink ports.

DigitalMedia IP Configuration

The following considerations should be followed when configuring DigitalMedia devices over IP.

Private Network Mode

PNM (Private Network Mode) greatly reduces the number of IP addresses required for DigitalMedia installations. Crestron recommends using PNM to manage Ethernet settings for DM cards and endpoints connected to a DM switcher. Other methods are not recommended. For details on legacy modes of operation, refer to Crestron True Blue Online Help.

> **NOTE:** PNM is not applicable to standalone installations involving directly connected DM endpoints with no associated DM switchers. In these installations, each endpoint device needs its own IP address, either configured manually or via DHCP.

PNM creates a completely private IP network for all DM cards and endpoints that are connected to the DM switcher, effectively isolating them from the building network. PNM significantly streamlines home and organizational infrastructures, conserves IP addresses, reduces costs, and simplifies system management and troubleshooting.

The only device that appears on the building network is the DM switcher. The switcher needs just one IP address, which can either be set statically or assigned via the building's DHCP server. In PNM mode, none of the cards or endpoints are directly reachable via the network of the building. Instead, communication with these devices is managed through the main DM switcher. The devices connected to the LAN ports found on many DM endpoints remain visible to the network. Refer to Private Network Mode with Auxiliary Devices on page 15 for an illustration.

The main DM switcher CPU is the only device connected to both networks. The CPU may receive an instruction on the public network (such as from a Crestron control system) and create a new instruction for a device on the private network (DM card, blade, or endpoint). At no time does an Ethernet packet from the public network traverse to the private network, and no private Ethernet packets traverse to the public network.

For most installations, such as in corporate or university settings, using PNM is the best practice because it does not heavily impact the network. PNM also isolates DM-related traffic.

NOTES:

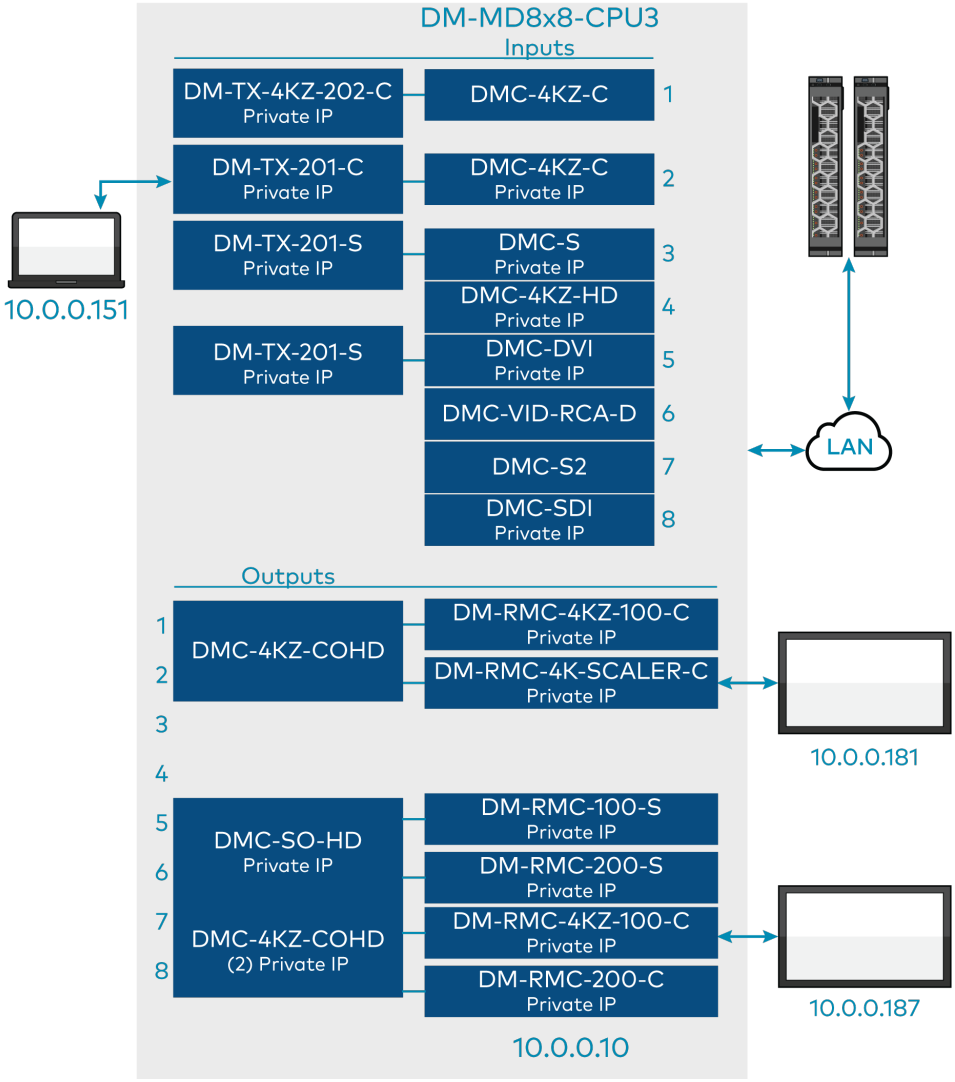
- PNM is enabled by default on all new units and is enabled upon system restore. PNM is only available in PUF (firmware package update file) 2.40 or later.
- PNM is not configurable on switchers equipped with the DMC-CPU3, where it is always enabled.
- DMPS units require two IP addresses. Both the integrated control processor and the integrated DM equipment (switcher and all endpoints) require their own IP address.
- If an endpoint is connected to a DM switcher, its LAN connector must not be connected to the corporate network. In this configuration LAN ports are only for connection to devices such as laptops, Blu-ray Disc™ players, or projectors.

Private Network Mode Configuration Options

PNM ON/OFF	Mode	Comments
PNM ON	Static	Assigns one IP address to the main DM switcher
PNM ON	DHCP	Takes one IP address from the DHCP server
PNM OFF*	Static and DHCP	Can be in Static or DHCP mode Requires many IP addresses Not recommended for most installations

* Applies to DM-MD8X8, DM-MD16X16, and DM-MD32X32 with DMC-CPU only. PNM is not configurable on switchers equipped with the DMC-CPU3, where it is always enabled.

Private Network Mode with Auxiliary Devices



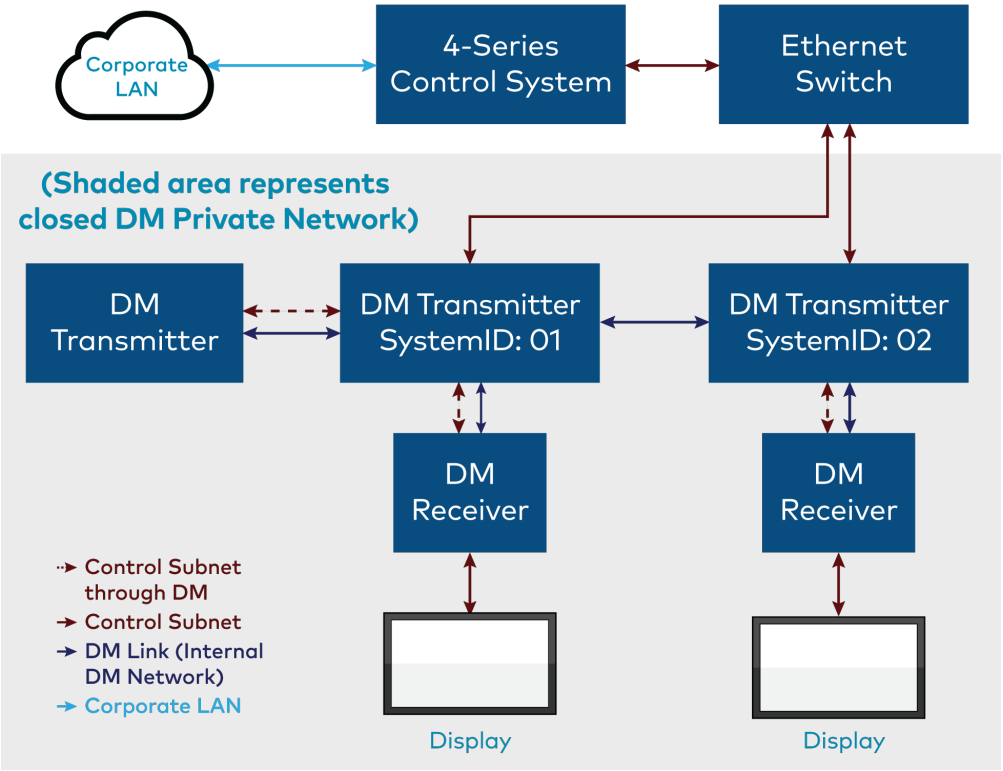
NOTES:

- DHCP-distributed IP addresses have been chosen at random to show that devices attached to DM endpoints are connected to the building LAN.
- The laptop in the example receives an IP address from the DHCP server.
- The devices enclosed in the gray box are isolated from the customer network but are accessible through the IP address assigned to the DM-MD8X8(-CPU3).

Multiple DigitalMedia Switchers Using Private Network Mode

When two or more switchers are connected via DM links, they are considered cascaded. Each DM switcher in a cascaded system must be configured with a unique SystemID. This prevents IP conflicts among DM devices on the private network. In the illustration below, only one IP address per switcher is required from the building network.

Multiple DM Switchers Using PNM Example



NOTE: The SystemID can range from 01 to 64 and must be unique for each DM switcher. By default, the SystemID is set to 01. The ID can be set via the front panel, the SIMPL program, or the System Info tool in Crestron Toolbox. Each DM switcher must be directly connected to the corporate LAN. One DM switcher cannot receive Ethernet via another DM switcher, and each DM switcher must receive an IP address from the control subnet.

Rapid Spanning Tree Protocol

Since DM devices embed Ethernet in every link, a valid AV configuration can create network loops, such as routing two AV signals from one switcher to another switcher. To eliminate any network looping problems, DM products implement IEEE 802.1w RSTP (Rapid Spanning Tree Protocol). With PNM enabled, the DM switcher manages the DM Ethernet links to prevent network loops.

DM products transmit Bridge Protocol Data Units (BPDU) per the RSTP specification. With PNM enabled, BPDUs are isolated to the private network and are not visible to the corporate network. RSTP is not enabled on user-accessible LAN connectors. To prevent network loops, endpoints should not be connected to the corporate LAN in this configuration.

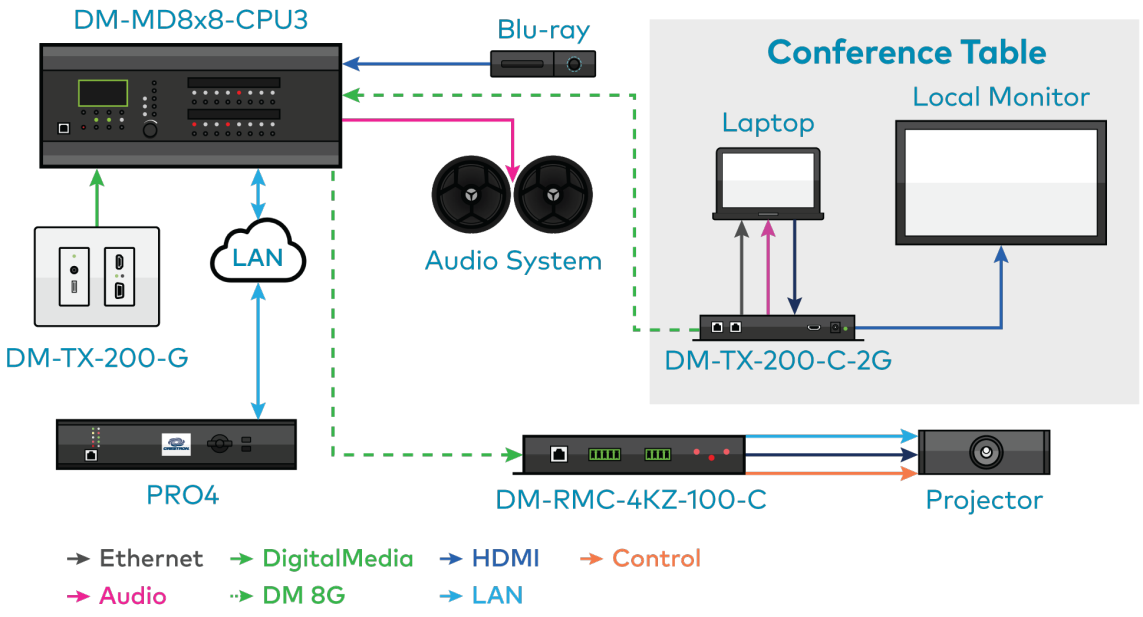
By default, every DM switcher ships with PNM and RSTP enabled. If PNM is disabled, RSTP remains enabled. If required, disable RSTP and manage Ethernet ports manually.

> **NOTE:** PNM is not configurable on switchers equipped with the DMC-CPU3, where it is always enabled.

Multiple Spanning Tree Protocol (MSTP), which is an advanced version of RSTP, supports multiple spanning trees on multiple VLANs. DM implements RSTP but not MSTP. If running MSTP on the network, ensure that the network port to which DM is connected only belongs to one VLAN. This is only a problem if PNM is disabled.

Managed Ethernet switches can be configured to have edge ports. Ethernet switches cannot be plugged into edge ports. If PNM is enabled, a DM switcher is compatible with edge ports. If PNM is disabled, the managed Ethernet switches may consider the DM system to be an Ethernet switch and shut down the edge port.

DM Ethernet Wiring Example



NOTES:

- DM switchers should be the only devices in the DM system connected to the LAN.
- Ensure that the SystemID of each DM switcher in the system is unique.
- Do not connect room controllers or transmitters to the LAN.

Power over Ethernet Budgeting

Power over Ethernet (PoE) provides a one-wire solution for connecting Crestron touch screens, gateways, and other devices. PoE delivers power and data over a single CAT5 (or greater) network cable. All five ports are Gigabit capable to ensure maximum bandwidth for multimedia and critical control data.

The PoE standard specifies power by class. When connected to Power Sourcing Equipment (PSE), each Powered Device (PD) declares its class to the PSE. The PSE in turn reserves a set amount of power for each device based on its class, as shown in the table below.

Class	Power Range
Class 0 (Unclassified)	Up to 15.4 W at PoE port, 12.95 W at device
Class 1	4.0 W at PoE port, 3.84 W at device
Class 2	7.0 W at PoE port, 6.94 W at device
Class 3	15.4 W at PoE port, 12.95 W at device
Class 4 (PoE+)	30.0 W at PoE port, 25.50 W at device

Power Budgeting on PoE Switches

The calculation for power budgeting on PoE switches is :

Number of Class 0 devices: _____ x 15.4 = _____
Number of Class 1 devices: _____ x 4.0 = _____
Number of Class 2 devices: _____ x 7.0 = _____
Number of Class 3 devices: _____ x 15.4 = _____
SUM of LLDP PSE wattages for Class 4 devices = _____

Total _____

PoE switches reserve the maximum of each classification regardless of how much power the device is actually using. Class 4 (PoE+) is for devices that range from 13 to 25.5 W.

PoE+ powered devices are required to support Link Layer Discovery Protocol (LLDP) power negotiation. If the PoE+ switch supports this, the amount of power reserved is negotiated between the switch and the device. Consult the data sheet for the device to determine the PoE+ power required. The CEN-SWPOE-16 implements LLDP power negotiation. LLDP negotiation is optional per the 802.3at standard for power source equipment. Therefore, if the PSE does not support LLDP negotiation, the full 30 watts is reserved for all Class 4 devices.

IEEE Standards

The IEEE 802.3at standard has replaced 802.3af. The 802.3af standard preceded PoE+ and only covers Classes 0 through 3. The 802.3at standard covers Classes 0 though 4.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7656
www.crestron.com

Best Practices — Doc. 4579P
04/05/24
Specifications subject to
change without notice.