DigitalMedia™ NVX System

Design Guide

Crestron Electronics, Inc.

HDMI

This document was written by the Technical Publications department at Crestron.

Contents

DigitalMedia™ NVX System

Introduction

A Crestron® DigitalMedia™ NVX system is a digital video and audio distribution system that switches 4K video sources and displays at 60 frames per second (fps) with full 4:4:4 color sampling and High Dynamic Range (HDR) video support. Using standard 1-Gigabit Ethernet infrastructure, a DM® NVX system provides a highly flexible, cost-effective, and infinitely scalable network AV solution without loss of quality. Using JPEG2000 wavelet-based compression, a DM NVX system encodes and then simultaneously decodes and scales, eliminating any latency incurred when transmitting video over the network.

A DM NVX system offers a combined encoder/decoder endpoint design in surface-mountable and card-based form factors. In addition, the DM XiO Director™ network appliance can be added to configure, control, and manage a DM NVX system.

This guide aids in the design and installation of a DM NVX system. The guide provides information about the following:

- System design, which includes endpoint and network design
- System installation, which includes endpoint and network installation
- Case studies

In addition, a glossary is provided at the end of the guide.

System Design

The following sections provide design information related to DM NVX endpoints and the network.

Endpoint Design

A DM NVX system is composed of one or more encoder endpoints and one or more decoder endpoints. Each endpoint is configurable to operate as either an encoder (transmitter) or decoder (receiver).

Additional components of a DM NVX system include the DM XiO Director network appliances and SFP (Single Form-factor Pluggable) transceiver modules.
SFP transceiver modules can be used with the endpoints and network appliances to add fiber connectivity.

The following sections provide information about DM NVX endpoints, DM XiO Director network appliances, SFP modules, and related system design considerations.

DM NVX Endpoints

An overview of the hardware and features of the DM NVX endpoints follows.

Hardware Overview

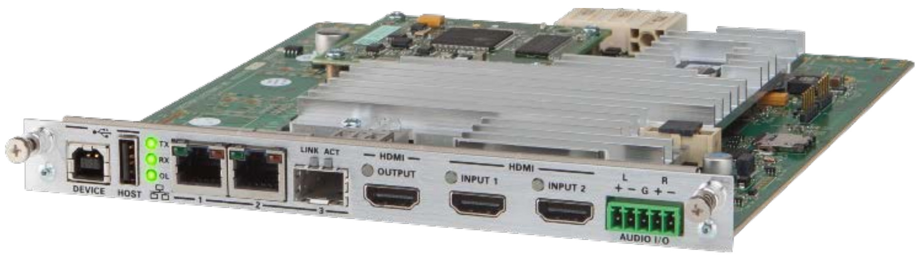
Two types of DM NVX endpoints are available:

1. Stand-alone endpoints, which consist of the DM-NVX-350 and the DM-NVX-351. The compact design allows the endpoints to fit easily in various types of locations, for example, behind a flat panel display.
2. Chassis-based cards, which consist of the DM-NVX-350C and the DM-NVX-351C. The cards are used with the DMF-CI-8 card chassis for sources in close proximity to a rack or for applications requiring a high density of endpoints.

DM-NVX-350 and DM-NVX-351 Front Panel

DM-NVX-350 and DM-NVX-351 Rear Panel

DM-NVX-350C and DM-NVX-351C Front View



Stand-alone and chassis-based endpoints provide the following physical connectivity:

- Two switchable local HDMI® inputs for 4K 60 fps 4:4:4 HDR video and multichannel audio
- One local HDMI output for 4K 60 fps 4:4:4 HDR video and multichannel audio
- One analog stereo balanced line-level input and output audio port for local insertion of audio, replacement of HDMI audio source, or output of audio
- Two 1-Gigabit Ethernet RJ-45 ports that support a transmission distance of up to 330 feet (100 meters) over shielded or unshielded Cat 5e or higher cable
- One 1-Gigabit Ethernet SFP port for optional fiber-optic connection using Crestron SFP-1G transceiver modules
- One USB 2.0 host port for connecting keyboards, mice, and other peripherals
- One USB 2.0 device port for connecting a USB host such as a PC

Only stand-alone endpoints provide the following physical connectivity:

- One serial RS-232 computer console port for device setup
- One USB 2.0 computer console port for device setup
- Two IR/serial output ports for device control
- One COM port for RS-232 communication

Stand-alone endpoints also include setup, reset, and input selection push buttons for manual control.

Features

Features available on all stand-alone and chassis-based endpoints include the following:

- **Integrated Security**: Endpoints integrate security features, which include 802.1X using TLS or MS-CHAP v2 authentication, Active Directory® service support for endpoint management, audio and video stream encryption, secure Crestron IP device control, and secure device console access.
- **CEC Control**: Consumer Electronic Control messages are passed between endpoints, allowing for easy control of source and display devices that support CEC.
- **USB Routing:** USB 2.0 data is routed from one DM NVX endpoint to another and is independent of video and audio routing. One endpoint must be configured as a USB host, and the other endpoint must be configured as a USB device.
- **3D Surround Audio Support**: Endpoints can pass audio for 3D speaker configurations as well as traditional 5.1 and 7.1 multichannel surround audio with lossless audio support. A DM-NVX-351 or DM-NVX-351C must be used to generate a stereo downmix.
- **Secondary Audio**: Encoders can generate a secondary audio stream that is routed independently of the primary AV stream. The secondary audio stream is stereo LPCM only. If primary audio is multichannel content, a DM-NVX-351 or DM-NVX-351C is required to downmix for the secondary audio stream.
- **LAN Port Switch**: A built-in three-port LAN switch is connected to the two RJ-45 ports and one SFP module cage, enabling daisy chaining of endpoints and control of third-party devices in addition to primary DM NVX video stream input and output.
- **Power over LAN**: A built-in RJ-45 LAN powered device (PD) port is compatible with the Crestron DM-PSU-ULTRA-MIDSPAN or other Crestron approved power injectors. The LAN port is also compatible with UPOE (Universal Power over Ethernet) network switches.
- **Video Wall**: Up to 64 displays can be daisy chained across endpoints to provide multidisplay video wall capability. Each endpoint provides fully customizable bezel compensation and zoom on any part of the source video.
- **Crestron XiO Cloud™ Service Connection:** The Crestron XiO Cloud service allows supported Crestron devices across an enterprise to be managed and configured from one central and secure location in the cloud. DM NVX endpoints are preconfigured to connect to the service. Use of the service requires a registered Crestron XiO Cloud account.

Endpoint Comparison

The following table summarizes the major differences among the DM NVX endpoints.

Major DM NVX Endpoint Differences

MODEL	FORM FACTOR	CARD CHASSIS REQUIRED	IR OUTPUT	COM (RS-232)	AUDIO DOWNMIX
DM-NVX-350	Stand-alone	No	Yes	Yes	No
DM-NVX-351	Stand-alone	No	Yes	Yes	Yes
DM-NVX-350C	Card	Yes	No	No	No
DM-NVX-351C	Card	Yes	No	No	Yes

DM XiO Director Network Appliances

A DM XiO Director enterprise-grade network appliance emulates the functionality of the traditional hardware-based matrix switcher (for example, the DM-MD8X8). The network appliance allows comprehensive system configuration, management, and signal routing of a DM NVX system.

A DM XiO Director network appliance provides a web interface that allows automatic discovery of each DM NVX endpoint on the network and the assignment of each endpoint to a domain. The DM XiO Director web interface also enables custom endpoint naming and search tools, an XML-based device map file for import and export, logging, diagnostics, and SNMP messaging support.

DM XiO Director models consist of the DM-XIO-DIR-80, DM-XIO-DIR-160, and DM-XIO-DIR-ENT. The following sections provide information about each model.

DM-XIO-DIR-80

The DM-XIO-DIR-80 includes four 1-Gigabit Ethernet RJ-45 interfaces and a dedicated Intelligent Platform Management Interface (IPMI). Best suited for single large rooms, the DM-XIO-DIR-80 supports 80 devices and a single domain.

DM-XIO-DIR-80 (Front View)

DM-XIO-DIR-80 (Rear View)

DM-XIO-DIR-160

The DM-XIO-DIR-160 includes four 1-Gigabit Ethernet RJ-45 interfaces and a dedicated IPMI. Best suited for groups of small rooms, the DM-XIO-DIR-160 supports 160 devices and 20 domains.

DM-XIO-DIR-160

DM-XIO-DIR-ENT

The DM-XIO-DIR-ENT includes six 1-Gigabit Ethernet RJ-45 interfaces, six 10-Gigabit Ethernet SFP+ interfaces (four of which are also compatible with 1-Gigabit Ethernet), a dedicated IPMI, and redundant power supplies.

DM-XIO-DIR-ENT (Front View)

DM-XIO-DIR-ENT (Rear View)

DM XiO Director Model Comparison

The following table summarizes the major differences among the DM XiO Director network appliances.

Major DM XiO Director Differences

MODEL	NUMBER OF NETWORK INTERFACES	MAXIMUM NUMBER OF DOMAINS	MAXIMUM NUMBER OF DM NVX DEVICES
DM-XIO-DIR-80	4	1	80
DM-XIO-DIR-160	4	20	160
DM-XIO-DIR-ENT	12	240	1,000

SFP-1G and SFP-10G Transceiver Modules

Crestron SFP-1G and SFP-10G transceiver modules provide fiber connectivity, which offers greater transmission distances than traditional copper. SFP-1G modules can be used with the DM NVX endpoints and DM-XIO-DIR-ENT. SFP-10G modules can be used with the DM-XIO-DIR-ENT. The following sections provide information about the modules.

SFP-1G Modules

Available SFP-1G modules consist of the following:

- **SFP-1G-SX**: 850 nm multimode fiber connections up to 550 m (1800 ft) over LC-terminated OM3 or OM4 fiber
- **SFP-1G-LX**: 1310 nm single-mode fiber connections up to 10 km (6.2 mi) using LC-terminated G.652 fiber
- **SFP-1G-BX-U**: 1310 nm/1490 nm single-mode fiber uplink connections up to 10 km (6.2 mi) using LC-terminated G.652 fiber
- **SFP-1G-BX-D**: 1310 nm/1490 nm single-mode fiber downlink connections up to 10 km (6.2 mi) using LC-terminated G.652 fiber

SFP-1G Modules

For each endpoint and for the DM-XIO-DIR-ENT, the connectivity options and the distance requirements determine the appropriate module that is to be used.

SFP-10G Modules

Available SFP-10G modules for the DM-XIO-DIR-ENT consist of the following:

- **SFP-10G-SR**: 850 nm multimode fiber connections up to 300 m (1000 ft) over LC-terminated OM3 and up to 400 m (1300 ft) over LC-terminated OM4 fiber
- **SFP-10G-BX-U**: 1270 nm/1330 nm single-mode fiber connections up to 10 km (6.2 mi) using LC-terminated G.652 fiber
- **SFP-10G-BX-D**: 1330 nm/1270 nm single-mode fiber connections up to 10 km (6.2 mi) using LC-terminated G.652 fiber

For the DM-XIO-DIR-ENT, the connectivity options and the distance requirements determine the appropriate module that is to be used.

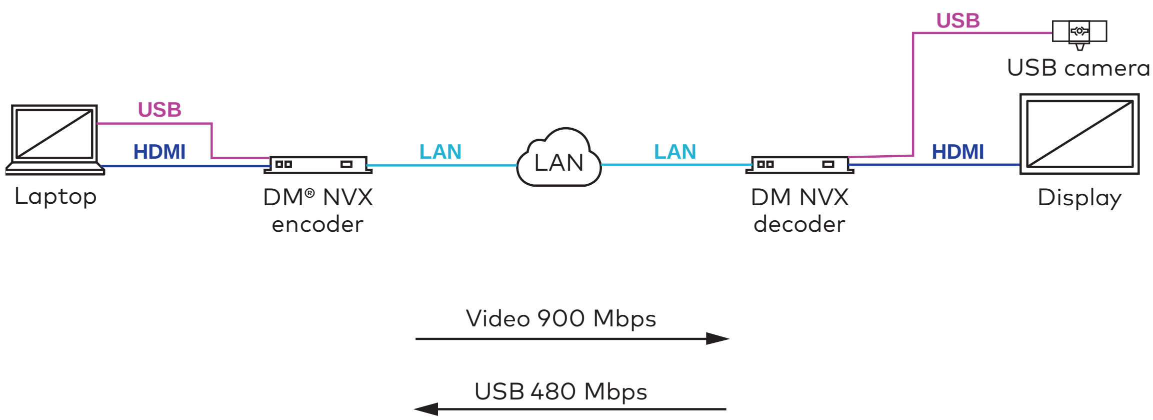
Endpoint Bandwidth Design and Management

A single DM NVX network link can carry the following data streams:

- **Primary Audio/Video Stream**: HDMI or analog audio and HDMI video that are encoded and sent to the network for decoding by a remote endpoint
- **Secondary Audio Stream**: Audio stream that is encoded and sent for decoding independently of the primary audio/video stream
- **USB Device and Host Traffic**: USB data from the DM NVX device or host port
- **Other Ethernet Traffic**: Control data as well as data from DM NVX network ports connected to third-party devices such as displays or cameras. Ethernet traffic also includes network protocol traffic such as DHCP, DNS, and RADIUS for 802.1X.

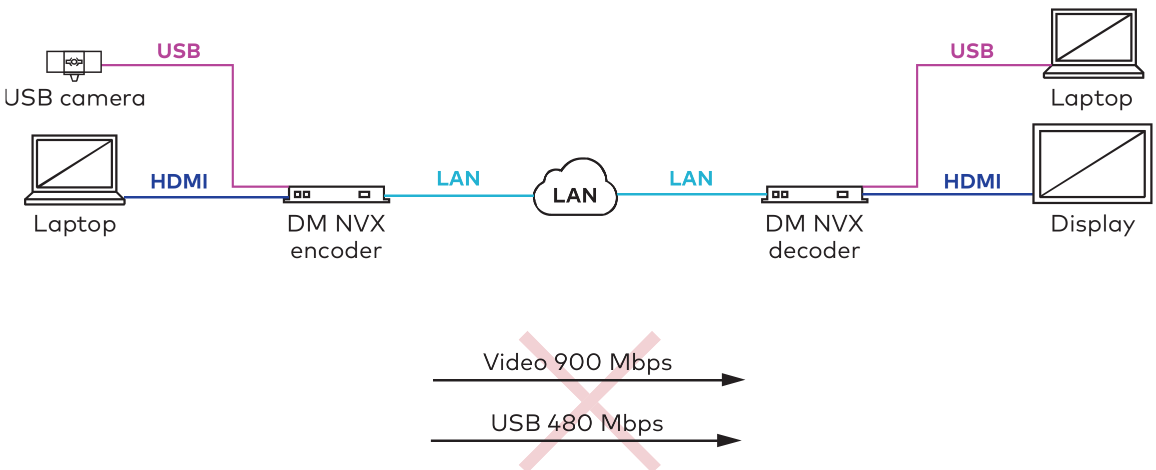
Default video bit rate settings are sufficient for most installations but can be adjusted to accommodate unique situations. Ethernet bandwidth ratings are bidirectional; therefore, full USB 2.0 bandwidth is supported. In a DM NVX installation in which video from a PC is encoded and sent to a decoder at a display, and a high-bandwidth USB camera at the display sends USB video back to the PC, no bandwidth issues exist. Although the sum of all traffic may exceed 1 Gbps in this scenario, the traffic in each direction is less than 1 Gbps.

Example of Bidirectional Bandwidth under 1 Gbps



An encoder that attempts to send 900 Mbps video and 480 Mbps USB 2.0 traffic exceeds the maximum network link bandwidth of 1 Gbps and, as a result, the link will fail.

Example of Failed Link with Required Bandwidth Greater than 1 Gbps



Endpoint Design Considerations

To implement an optimal configuration for a DM NVX system, consider the following factors for each endpoint:

- If rack-mount sources are required or if a high density of endpoints exists in close proximity to each other, use DM-NVX-350C or DM-NVX-351C card-based endpoints.
- If simultaneous stereo downmixing alongside multichannel audio output is required, use the DM-NVX-351 or DM-NVX-351C.
- Follow the guidelines for cable types as specified in TIA/EIA-568 for choosing and certifying cables in a DM NVX installation.
- Refer to the following table for guidelines on some of the primary network connectivity options that can be used at the endpoint.

Primary Endpoint-to-Network Connectivity Guidelines

CONNECTION	CABLE TYPE	MAXIMUM TRANSMISSION DISTANCE
RJ-45	Cat5e or higher	100 m (330 ft)
SFP-1G-SX	OM3 MMF OM4 MMF	550 m (1800 ft)
SFP-1G-LX	G.652 SMF	10 km (6.2 mi)
SFP-1G-BX-U	G.652 SMF	10 km (6.2 mi)
SFP-1G-BX-D	G.652 SMF	10 km (6.2 mi)

- As a courtesy feature, the DM-NVX-350 and DM-NVX-351 provide IR and serial ports to control in-room devices. Use a Crestron control processor— such as a PRO3 or AV3—in a design that uses IR and serial ports or in a design that requires relay I/O or Cresnet® device control.
- Although both the USB host port and USB device port are available on a DM NVX endpoint, only one of the ports can be used at a time.

- High-bandwidth USB devices such as cameras and storage can have an impact on overall video bandwidth. For additional information about how to manage high-bandwidth USB devices and the direction of bandwidth consumption, refer to "Endpoint Bandwidth Design and Management" on page 8.
- If additional HDMI inputs are required for local switching at the endpoint within typical HDMI cable distances of 15 ft (5 m), consider using other Crestron solutions—such as the Crestron DM MD and DMPS families of products—in conjunction with the endpoint.
- In many DM NVX installations, configure specific control surfaces (such as Crestron touch screens) and additional switch options (such as local HDMI switches) at endpoints.

Network Design

DM NVX systems require a designed and provisioned Ethernet network to function correctly. Be sure to gather requirements and documentation, coordinate with IT staff, and complete network design prior to site work.

Network Design Overview

DM NVX networks must be designed to isolate traffic on network segments specifically architected for DM NVX devices. This can be accomplished by using separate infrastructure, Virtual Local Area Networks (VLANs), or Multi-Protocol Label Switching (MPLS). DM NVX network segments carry DM NVX multicast streams, DM NVX control, and ancillary traffic.

The location of other Crestron network devices relative to network infrastructure must be determined. A decision must be made as to whether the devices are to coexist on the same network segment as the DM NVX segment or on another segment that has traversal capabilities to the DM NVX segment but is not multicast enabled. Networked AV devices other than DM NVX devices can be placed on the DM NVX network segment if their bandwidth requirements are relative to the DM NVX endpoint bandwidth requirements.

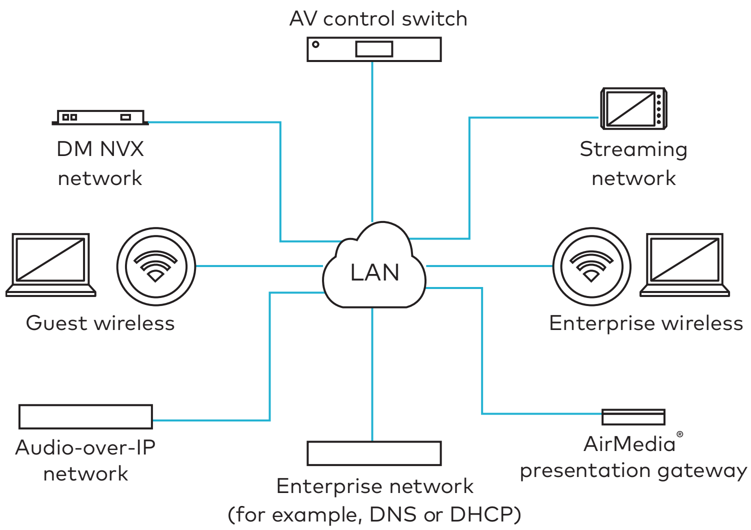
A DM NVX device can have up to three addresses:

- The first address is required for control of the device and access to the web configuration interface and console.
- Two additional addresses are required for multicast streams: one address for the primary multicast stream of audio and video and another address for the secondary audio multicast stream.

  During endpoint configuration, the primary multicast address must be set manually to an even-numbered IP address. The secondary audio multicast stream address can be automatically assigned to a value of one higher than the primary IP multicast stream address or can be manually set to the desired multicast address.

The DM NVX network segment must receive network services, including DNS, DHCP, Active Directory, and RADIUS services. Coordinate with IT staff to provide access to these services and to create the proper traversal rules to the DM NVX network segment.

Network Segmentation along Logical Boundaries



Consideration must be given to blocking at both the switch level and the network design level. DM NVX network switches must have enough switch fabric bandwidth to support full nonblocking bidirectional gigabit bandwidth on all ports simultaneously. This is a common feature in enterprise-grade gigabit network switches, but it should not be assumed that a switch is nonblocking or is configured as nonblocking.

Due to system size or physical layout, most DM NVX installations require multiple network switches. The network switches must connect to each other via a high-bandwidth uplink port. For network design purposes, assume that each DM NVX link consumes the full gigabit of link bandwidth.

Consider the example of a standard 48-port Gigabit Ethernet switch with one 40-gigabit uplink (or four 10-gigabit uplinks). Since each DM NVX endpoint consumes 1 gigabit of bandwidth, this switch can support up to 40 DM NVX devices in a nonblocking way. If more devices are connected, the uplink becomes a bottleneck, introducing the potential for difficult-to-diagnose blocking problems.

Network Topologies

Connect devices such as control processors, touch screens, servers, personal computing devices, and DM NVX endpoints directly to network switches. In a large network with multiple layers of switch hierarchy, situate these devices at the network's edge. The network edge switches are often connected via uplinks to other switches and routers. This aggregates traffic from the network edge and forms the network's core. The relationships between network switches and their interconnection to each other define the network's topology.

The following general rules apply for sizing network switches in terms of switch fabric nonblocking bandwidth:

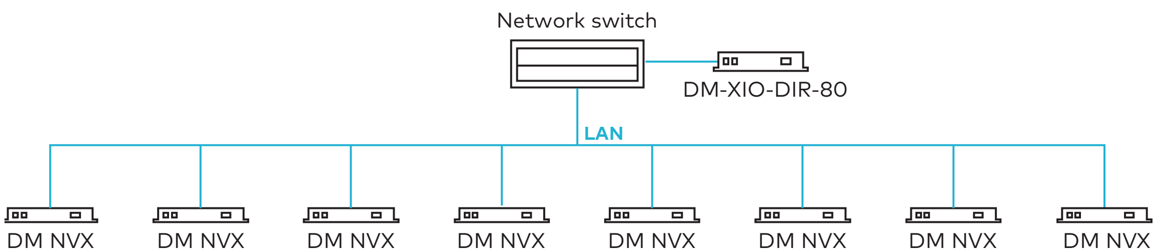
- The network core must support a nonblocking bandwidth and port speed equal to 1 gigabit multiplied by the lesser of the total number of anticipated encoder endpoints or the total number of anticipated decoder endpoints, plus the number of USB extenders.
- The network edge must support a nonblocking bandwidth and uplink speed equal to 1 gigabit multiplied by the greater of the total number of anticipated encoder endpoints or the total number of anticipated decoder endpoints, plus the number of discrete USB extenders.

Star

The default recommended network topology is a star. Using a fully nonblocking switch, the star topology allows any combination of one or more endpoints to connect to any other combination of endpoints. It also easily allows the network to grow beyond a single switch if the uplink in the switch supports the maximum specified bandwidth.

For small DM NVX systems that employ only one network switch, use a nonblocking switch to prevent a bottleneck. Star topologies can accommodate very large DM NVX installations by using large modular switch frames.

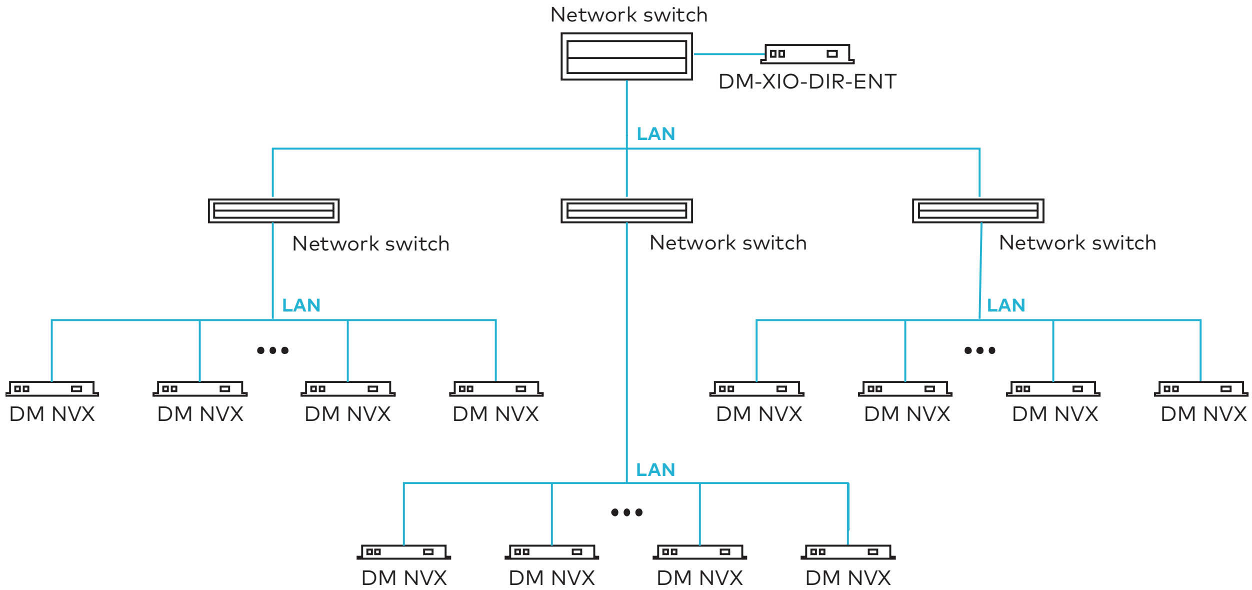
Star Network Using a Nonblocking Switch



Tree

A tree network is a combination of more than one star network existing on a core-switching infrastructure. The tree network allows failure in one part of the attached star networks without widely affecting the other star networks.
Configure the core network, which is the larger network switch, for redundancy and scalability.

Tree Topology Using Nonblocking Switches on a Core Network



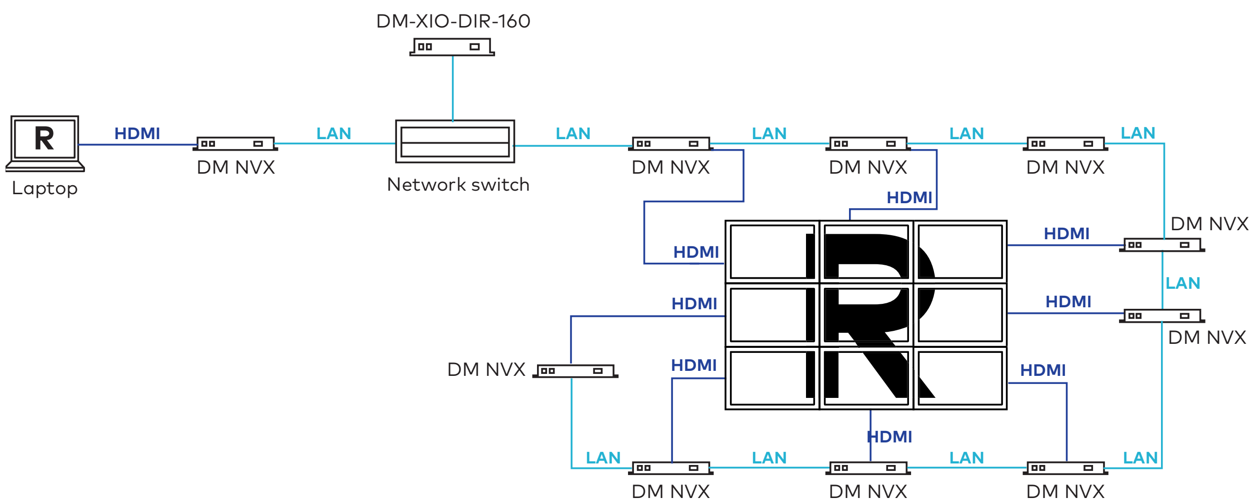
Daisy Chain

Daisy chaining is appropriate for specific deployment applications such as video walls or jury boxes in which all displays receive the same video source as the first DM NVX endpoint in the chain.

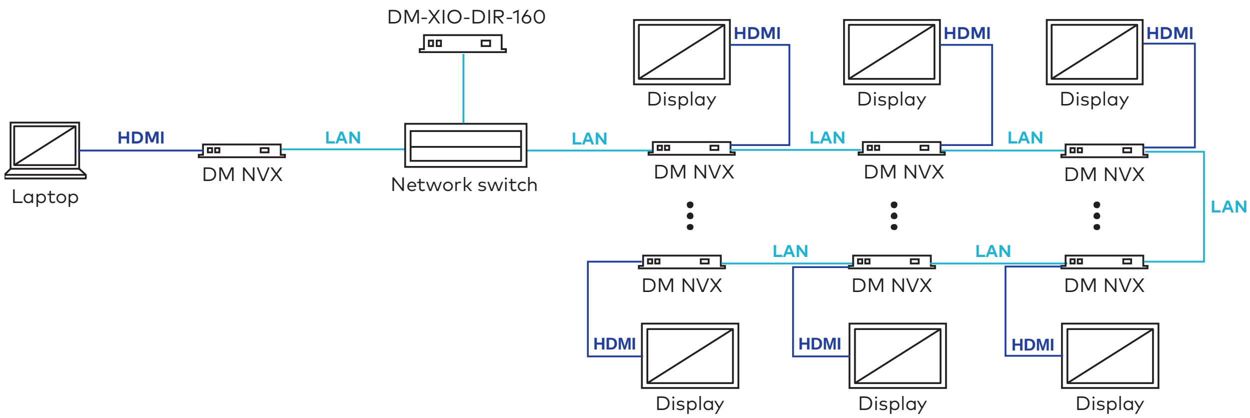
For video wall applications and any other application in which displays are near each other and share the same source, up to 16 endpoints can be daisy chained together. Larger video walls can be divided into individual daisy chains that each contain up to 16 endpoints.

For applications such as information signage in which more than one display is viewable concurrently without being dependent on the viewing of another display in the daisy chain, up to 64 endpoints can be daisy chained together.

Daisy Chain Network Configuration for 3 x 3 Video Wall



Daisy Chain Network Configuration for 12-Person Jury Box



Due to limited bandwidth for audio and video, a USB host or device on a daisy chained endpoint is not recommended. For maximum flexibility and the ability to reconfigure video walls with multiple sources, connect DM NVX endpoints directly to switches rather than daisy chain the endpoints.

Other Topologies and Network Functionality

Other valid deployment topologies for DM NVX networks are ring and mesh. These deployments require project-specific discovery and configuration of the network switch. For projects using advanced topologies for deployments, a networking professional must be involved early in the network design process.

Network Multicast Functionality

DM NVX networks rely on multicast functionality to send and receive video—even in the simplest case of a single encoder endpoint and a single decoder endpoint. Internet Group Management Protocol (IGMP) multicast in the Ethernet context replaces a fixed switching architecture in AV distribution.

Segregation of DM NVX traffic by using a VLAN or MPLS is usually the first step in enabling multicast. A VLAN or MPLS ensures that DM NVX traffic stays on the DM NVX network and does not route to other network segments and interfere with their operation. A VLAN or MPLS also ensures that traffic from other network segments does not interfere with DM NVX operation. Within that segment, all ports can be flooded by IGMP traffic regardless of whether that traffic was intended to be sent or received by a network device at any time. This will result in interference with network operation and can be a means of implementing a denial-of-service attack on a network if done maliciously.

To ensure that only traffic between intended multicast senders and multicast receivers appears at a given port, IGMP snooping must be enabled. IGMP snooping refers to the ability of the network switch to limit multicast traffic only to ports between intended senders and receivers. The DM NVX network supports both versions of IGMP snooping: IGMPv2 and IGMPv3.

In order for the network switch to know where route limiting is implemented in the network for multicast traffic, an IGMP querier must be enabled. In most instances, a single network switch is selected by address to act as the IGMP querier; however, if multiple switches are configured as queriers, the switch with the lowest numerical IP address on the network is typically the default. The default leave time for the querier (typically about 125 seconds) is sufficient for a DM NVX network.

Protocol Independent Multicast (PIM)

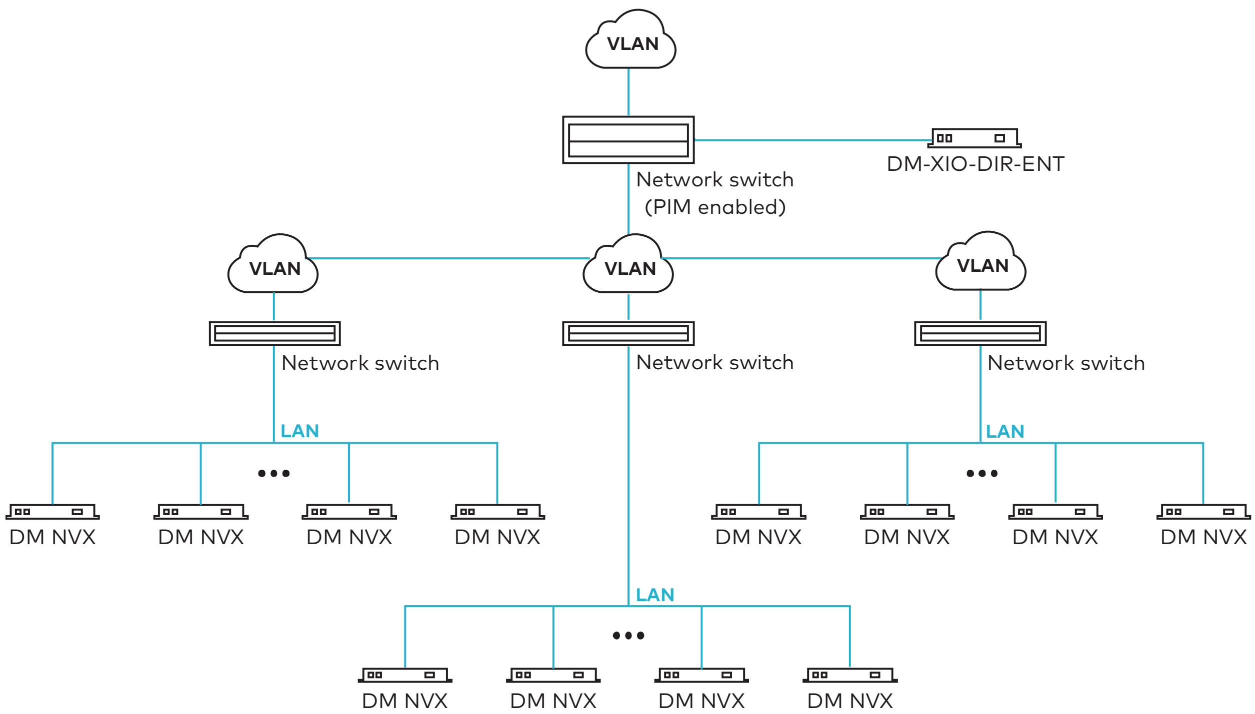
Protocol Independent Multicast (PIM) is a family of multicast routing protocols for IP networks. PIM offers one-to-many and many-to-many distribution of data. PIM modes include PIM Sparse Mode (PIM-SM), PIM Dense Mode (PIM-DM), and PM Source-Specific Multicast Mode (PIM-SSM). PIM-SM must be used for large DM NVX networks. PIM-SM finds the shortest trees per path from a multicast source to multicast receivers on a network and is more scalable than PIM-DM or PIM-SSM. PIM-SM also prevents edge-to-switch link saturation and network loops in multicast traffic routing.

Enabling network Quality of Service (QoS) helps prioritize DM NVX traffic over other traffic at both the source and the destination. The highest priority on IGMP multicast traffic must be enabled. An example of enabling network QoS is as follows:

1. Enable 802.1Q VLAN tagging support in the network switch.
2. Enable and assign an 802.1P priority (for example, 5, 6, or 7) to DM NVX addresses and ports or IGMP protocol traffic.
3. For other traffic, such as HTTP for web services or SSH for console access, assign lower priority numbers (for example, 0 to 4) based on their addresses, ports, or protocols.
4. For successful QoS operation, ensure that all traffic types are included in the QoS setup.

NOTE: In addition to 802.1Q and 802.1P mentioned on the preceding page, other QoS protocols exist and are dependent on the switch vendor. The protocols are configured similar to the 802.1Q and 802.1P examples on the preceding page.

PIM Multicast Routing Protocol for an IP Network



Network Security

Security requires the support of particular capabilities within all devices on the network. DM NVX networks employ the following security features:

- 802.1X authentication is used to ensure that devices on the network have been authorized by the network administration team. Unauthorized devices are prevented from being added to the network and from having access to sensitive content.
- Active Directory services for endpoint administration can be used to ensure that administrative privileges for DM NVX devices can be centrally managed, granted, and revoked when necessary.
- DM NVX endpoints use Advanced Encryption Standard (AES) block cipher with Public Key Infrastructure (PKI) for stream encryption to protect content from unauthorized access as it crosses the network.
- SSL-based secure Cresnet over IP (CIP) for DM NVX control ensures that control processors and DM NVX devices communicate with the intended party device and that any unauthorized device on the network cannot monitor commands and status.
- SSH-based command line console access for device configuration and status protects the device console from access by unauthorized users.

SSL-based Cresnet over IP and SSH-based command line console access are automatically configured within DM NVX devices and support software. The designer should focus on 802.1X and Active Directory services within the design.

For additional information about deploying security with Crestron products, refer to the IP Considerations Guidelines for the IT Professional Design Guide (Doc. 4579) at www.crestron.com/manuals and to Answer ID 5571 in the Online Help section of the Crestron website (www.crestron.com/onlinehelp).

Network Design Considerations

Consider and apply the following network design best practices:

- Use nonblocking Layer 3 switches with port-based QoS such as 802.1P with 802.1Q at all stages of the design. Use sufficient switch bandwidth and port speeds. Less expensive switches cause loss of capability in the network.
- Choose switches with sufficient bandwidth at each segment—from edge to core—to accommodate a nonblocking architecture for DM NVX endpoints and any additional needs.
- Choose an appropriate network topology. Consider the network, including basic functionality and redundancy, and whether video walls or repetitive display signage is necessary. When planning a topology for the network, ensure that network IT staff and network architects are involved in the decisions.
- Enable an IGMP querier on at least one switch in the DM NVX network. The IGMP querier ensures that all switches know which multicast transmitters and receivers are connected to which switches in the network. Enabling an IGMP querier on multiple switches causes the switch with the lowest value of IP source address to take priority and act as the querier.
- Consult the network switch manufacturer's documentation to ensure that the uplinks are properly configured to support multicast traffic.
- Use switches that support 802.1X for endpoint authentication by implementing 802.1X endpoint authentication through TLS or MS-CHAP v2. Only authorized endpoints can communicate with the network.
- Ensure that VLANs or MPLS are implemented correctly. Leveraging existing switch infrastructure with VLANs or MPLS can cause conflicts with network provisioning needs. If a dedicated DM NVX network is not going to be used, VLANs must be implemented correctly with their own IP subnet, and MPLS networks must be configured correctly.
- Account for even-numbered DM NVX primary stream multicast address assignments since both primary and secondary multicast streams are possible. The assignment of multicast IP addresses for primary streams should be even numbered to allow the secondary stream to be assigned to the odd-numbered IP address, which is one higher than the primary stream's IP address. For multicast IP address assignment, refer to the guidelines in IETF RFC 3171.
- Use the Active Directory service for administration security. Use of the Active Directory service with DM NVX endpoint logins allows for easy, seamless, and better controlled access from a central directory authority with fewer risks.

- Use a DHCP server with link-layer filtering, and configure the IP addresses of endpoints using DHCP rather than static IP addresses. Using a DHCP server with short lease times, MAC address filtering, and sufficient address space for future needs makes network management easier.
- Enable IGMPv2 (DM NVX default) or IGMPv3 multicast snooping on all switches in the DM NVX network. This is a requirement for all designs in order to enable multicast delivery to multiple endpoints. Without IGMP snooping enabled, switches that receive a multicast stream will transmit that stream to all ports simultaneously and saturate all network links.
- Use the Rapid Spanning Tree Protocol (RSTP) on the network to ensure that network loops are discoverable and to prevent deployment issues. Network management should account for RSTP discovery downtime when the network changes.
- Use and plan for DM XiO Director management of endpoints.
- Use daisy chaining to connect video wall endpoints or repeated displays. For video walls or endpoints that receive the same source from a single transmitter to feed multiple identical displays or in a video wall using a single source, it is simpler and less expensive to daisy chain the network.
- Disable IGMP proxy functionality on Crestron control processors with routers to ensure that DM NVX multicast traffic does not interfere with the control processor. The CP3N, Pro3, and AV3 control processors as well as DMPS3 presentation systems should have IGMP proxy functionality disabled when connected to the DM NVX network.
- Account for high-bandwidth external USB devices that are to be connected to DM NVX devices. Ensure that the bandwidth is accounted for as a separate 1-gigabit link since USB 2.0 bandwidth can consume 480 Mbps of the 1-gigabit link.
- Ensure that multicast IP addresses do not share the multicast MAC addresses. Sharing MAC addresses can cause network collisions and prevent normal operation of the DM NVX network.

System Installation

The installation phase should ensure that the interaction among designer, installer, programmer, and end user is considered in all installation decisions.

Endpoint Installation

Each DM NVX endpoint has unique installation requirements that depend on the following:

- Copper or fiber network connectivity of the endpoint
- Card-based or stand-alone endpoint

- Configuration of the endpoint as a transmitter or a receiver or whether the endpoint is to switch dynamically between modes
- Additional local HDMI inputs that require configuration
- Use of source autoswitching or external switching control
- Additional audio sources that require encoding
- USB device or host functionality
- Whether the endpoint is part of a video wall or goes to multiple identical displays
- Requirement for serial or IR control or both

For stand-alone and card-based endpoints, a Crestron touch screen can be linked through one of the spare LAN ports. The audio port can be repurposed to be a balanced line input for external analog audio input or for line output to a speaker system at the endpoint. The endpoint features and attached devices can be configured through programming or through the web interface.

Depending on the location of the control processor, serial and IR control of endpoint devices may be routed directly from that control processor. Access to HDMI and USB inputs and outputs can be provided through Crestron HDMI breakout devices for tabletops and walls.

Stand-alone endpoints can be mounted in any orientation as required. Typical locations for stand-alone endpoint mounting include inside closets and drop ceilings, underneath tables, and in podiums. The specific location is determined by the following factors:

- Length of HDMI and USB cable runs
- Location of display and audio devices, network connectivity, power for the device, and physical security requirements

Serial and IR connectivity can be run at longer lengths and are typically not drivers of the endpoint mounting location.

For card-based endpoints, the DMF-CI-8 card chassis is placed in a closet or locked rack near the source and display devices. (To ensure that the environmental conditions in the rack meet the specifications outlined, refer to the DMF-CI-8 product page on the Crestron website.)

The serial and IR interfaces are not provided by card-based endpoints. The functionality must be provided by other means, such as through a local Crestron control processor on the DM NVX network.

For a maintenance-free installation, follow these guidelines:

- While taking into account cable distances, plan the optimum location for the stand-alone or card-based endpoint—especially when distance-limited HDMI cables are involved.
- Avoid direct access to the endpoint by the end users. End users can induce failures or create a security risk due to unauthorized network access. Ensure that HDMI cables and wall plates are routed away from the endpoint appropriately.

- Use Category 2 certified HDMI cables to meet the minimum HDMI specifications at 4K or 1080p and to prevent problems such as degradation or loss of video or audio.
- Use properly terminated network cables. Network cabling must be either of the following:
  - Fiber that is terminated with a clean LC connector
  - Shielded or unshielded Cat 5e or higher copper cable that is terminated with an RJ-45 connector
- Observe the minimum bend radiuses and pull forces of cables to maintain cable integrity and prevent failures.
- Use plenum-rated cables in plenum spaces. Cables such as Crestron DigitalMedia plenum-rated cables are suitable. Fire-rated conduit for any fiber or copper cabling used in plenum spaces is also suitable.
- Practice good cable dressing—especially for card-based endpoints in racks.
- Manage EDID and HDCP proactively. For additional information, refer to the Crestron DigitalMedia System Design Guide (Doc. 4546) at www.crestron.com/manuals.
- HDR and deep color sources may not display correctly on endpoints with non-HDR or non-deep color displays. Ensure that the capabilities of the sources are matched to the capabilities of the displays.
- Use descriptive names for endpoints either through the DM NVX web interface or by replacing the default name in the Crestron Toolbox™ software. Do not rely on the default name or the Crestron IP ID.
- Physically secure the endpoint to a fixed point or rack to prevent movement over time. Secure all mounting points and mounting hardware for stand-alone endpoints, card chassis, and card-based endpoints.
- Leverage use of the DM XiO Director server for endpoint configuration. The presence of a DM XiO Director server makes it easy to configure and control multiple DM NVX endpoints on the network.
- Thoroughly document the installation of endpoints—including drawings, lists, and descriptions—in order to provide detailed information for those who are to maintain or upgrade the DM NVX network.

Network Installation

The installation of a DM NVX network varies greatly depending on a number of factors, including the following:

- Whether existing network infrastructure such as switches and cabling are to be reused
- Location of closets, racks, Intermediate Distribution Frames (IDFs), and Main Distribution Frame/Combined Distribution Frame (MDF/CDF) relative to the endpoints

For optimal installation and maintenance of the DM NVX network, follow these best practices:

- Use or repurpose existing infrastructure in DM NVX network installation cases.
- Use physical security for the network. Secure all network locations (MDF/CDF and IDF down to individual closets) from unauthorized access.
- Disable any unused ports on the network switches.
- Use a structured cabling approach such as those described in the TIA/EIA-568 standard. Include keystones in jacks and patch panels, shielded or unshielded solid copper conductor cable not exceeding 295 ft (90 m), and patch cables not exceeding 33 ft (10 m) to connect between patch panels. Use cable testers to verify the integrity of the installation and capacity for future expansion and backup.
- Use Crestron switch configuration files.
- Configure the routing of external servers. If nondedicated DHCP, RADIUS, Active Directory, or other servers are used, ensure that the servers access the DM NVX network.
- Thoroughly document all DM NVX network hardware and configurations.

Crestron Service Provider Handoff

Consult the Crestron Service Providers (CSPs) once the DM NVX network and endpoints are installed and interconnected. Typical activities of a CSP in a DM NVX installation may include the following:

- Writing appropriate control programs for controllers on the network
- Programming appropriate serial and IR control for endpoint devices
- Configuring external analog and digital audio source input and output
- Configuring video walls
- Designing button and UI features for control surfaces such as touch screens and switches
- Managing EDID for endpoint devices

As CSPs implement and deploy the program, installers and designers should test and review the functionality. The programmer must document the program functionality to avoid future issues.

Case Studies

This section provides the following case studies using DM NVX products:

- Case Study 1: Community College 4K AV Distribution Network
- Case Study 2: 4K Residential AV Distribution Network
- Case Study 3: 4K AV Distribution over Fiber

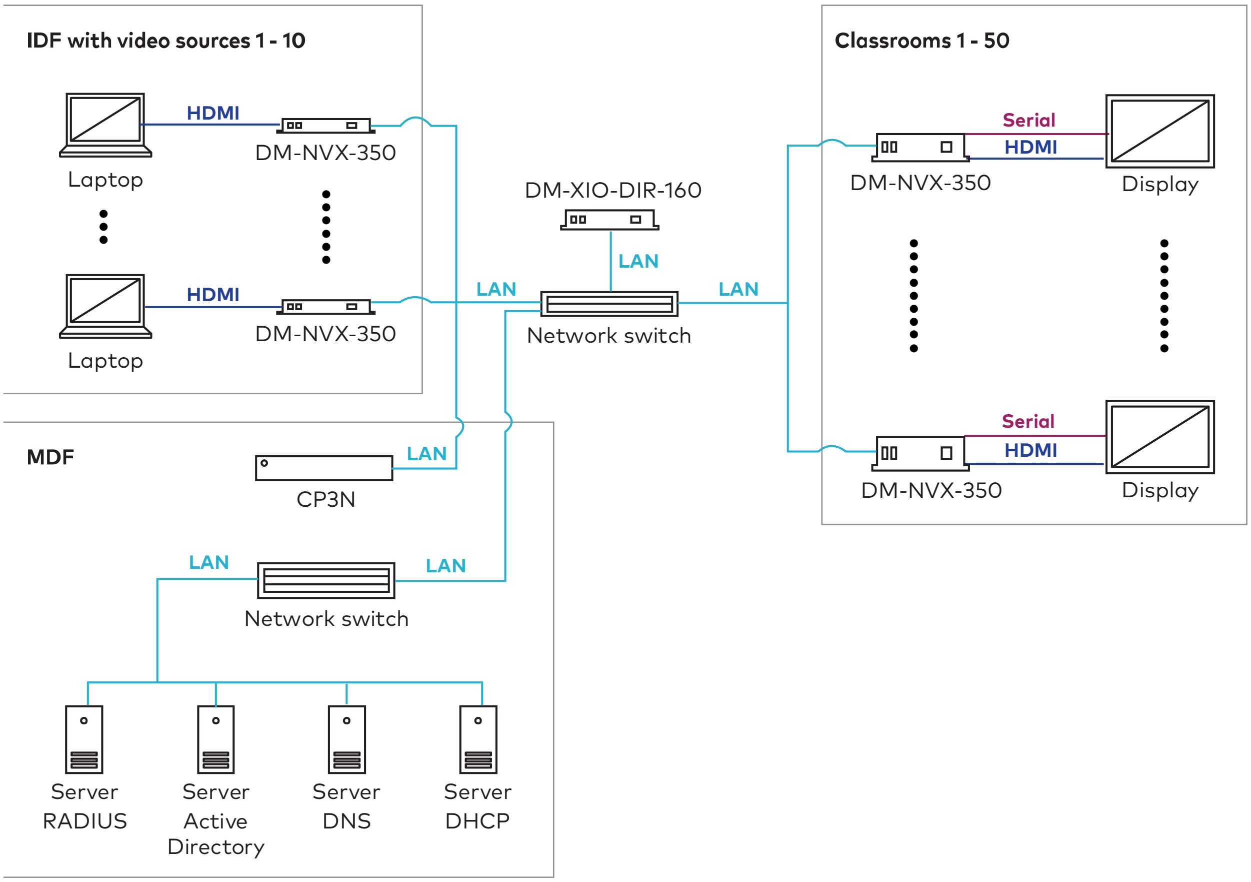
Case Study 1: Community College 4K AV Distribution Network

A client wants to distribute ten 4K HDMI video sources located in an IDF closet to 50 classrooms at a community college. More classrooms and 10 video sources are to be added in the future. The existing network cabling infrastructure is to be used—only the network hardware is required. External sound bars must be used for audio output at the displays.

Solution:

- The Crestron design is based on the use of DM-NVX-350 encoders and decoders and the DM-XIO-DIR-160:
    - Ten DM-NVX-350 encoders with video source connections are located in the IDF closet.
    - Each of the 50 classrooms has a DM-NVX-350 decoder that connects to a display. The DM-NVX-350 decoders feed video to the displays and provide serial control of the displays.
    - A DM-XIO-DIR-160 is used to set up, control, and monitor the DM NVX system. The DM-XIO-DIR-160 also provides the capability to add classrooms and ten video sources in the future.
- Using a star network topology, any source can be routed to any destination.
- The system can be controlled via the Crestron App for mobile and tablet devices.
- A Crestron CP3N control processor is installed in the MDF closet to provide centralized control for the entire system. Since no additional external control from the control processor is necessary, the processor connects directly to the network switch.
- A nonblocking network switch is used. The network switch has enough ports for 10 video source endpoints and 50 video display endpoints. In addition, the network switch can be reconfigured to support an additional 10 sources.

Case Study 1 Solution Diagram



Case Study 2: 4K Residential AV Distribution Network

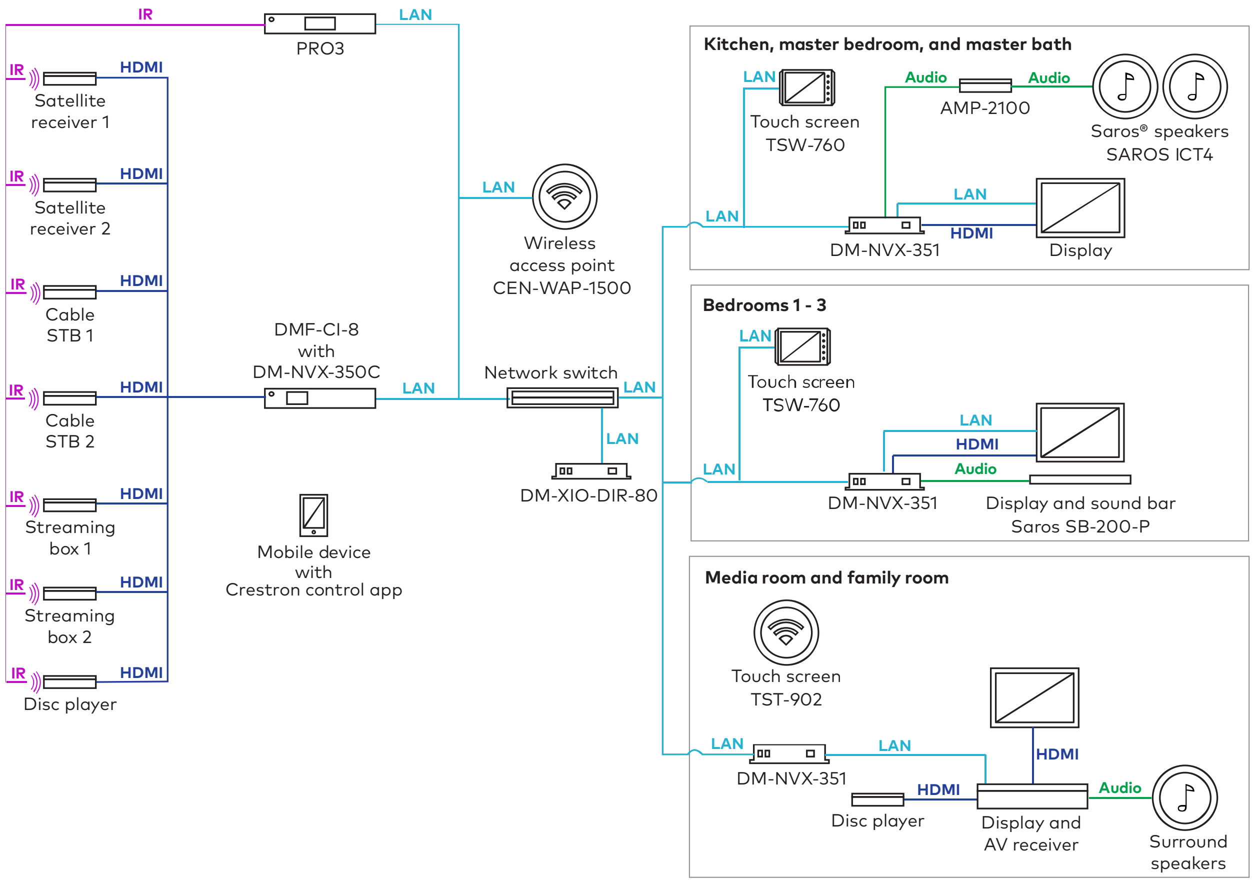
A privately owned home needs a retrofit 4K video distribution system. Sources are located in the basement rack room and are distributed to TV and surround sound receiver locations throughout the house. The desired system requires two satellite receivers, two cable set-top boxes (STBs), two streaming boxes, and one disc player. The media room and family living room require surround sound systems with a local 4K HDR Blu-ray™ player and 4K HDR displays. All other rooms require external speakers with stereo output. The kitchen, master bedroom, and master bathroom require in-ceiling speakers. Touch screens are the desired control surfaces. The media room and family living room are not able to have wire runs for the touch screens—only local power is available. Existing network infrastructure can be reused.

Solution:

- The Crestron design is based on the use of DM-NVX-350C cards as encoders, DM-NVX-351 stand-alone endpoints as decoders, and the DM-XIO-DIR-80:
  - Seven DM-NVX-350C cards are installed in a DMF-CI-8 chassis in the basement rack. Each of the seven video sources in the basement rack room connects to a DM-NVX-350C encoder.
  - The kitchen, master bedroom, and master bathroom each have a DM-NVX-351 decoder that connects to a display and provides audio downmixing. The stereo line audio output of a DM-NVX-351 connects to a two-channel amplifier with two Crestron Saros® IC4T in-ceiling speakers per room.
  - Bedrooms 1, 2, and 3 each have a DM-NVX-351 decoder that connects to a display and provides audio downmixing. The stereo line audio output of a DM-NVX-351 connects to a Crestron Saros SB-200-P sound bar.
  - The media room and family room each include a surround sound system that connects to a DM-NVX-351. The HDMI OUT from a surround sound system connects to a display. In-room speakers connect to the surround sound system.
  - A DM-XIO-DIR-80 is used to set up, control, and monitor the DM NVX system.
- The kitchen and three bedrooms each use a TSW-760 touch screen. The rooms can also be controlled using the Crestron App for mobile and tablet devices.
- Due to a cable routing constraint, the media room and family room each have a TST-902 wireless touch screen for control. The rooms can also be controlled using the Crestron App for mobile and tablet devices.
- A Crestron PRO3 control processor with expansion cards controls the entire system by providing IR and other peripheral control.

- Using a star network topology, any source can be routed to any destination.
- A Crestron specified network switch is used. The network switch has enough ports for seven video source endpoints and five video display endpoints.
  In addition, the network switch can be reconfigured to support future expansion for newer sources.

Case Study 2 Solution Diagram



Case Study 3: 4K AV Distribution over Fiber

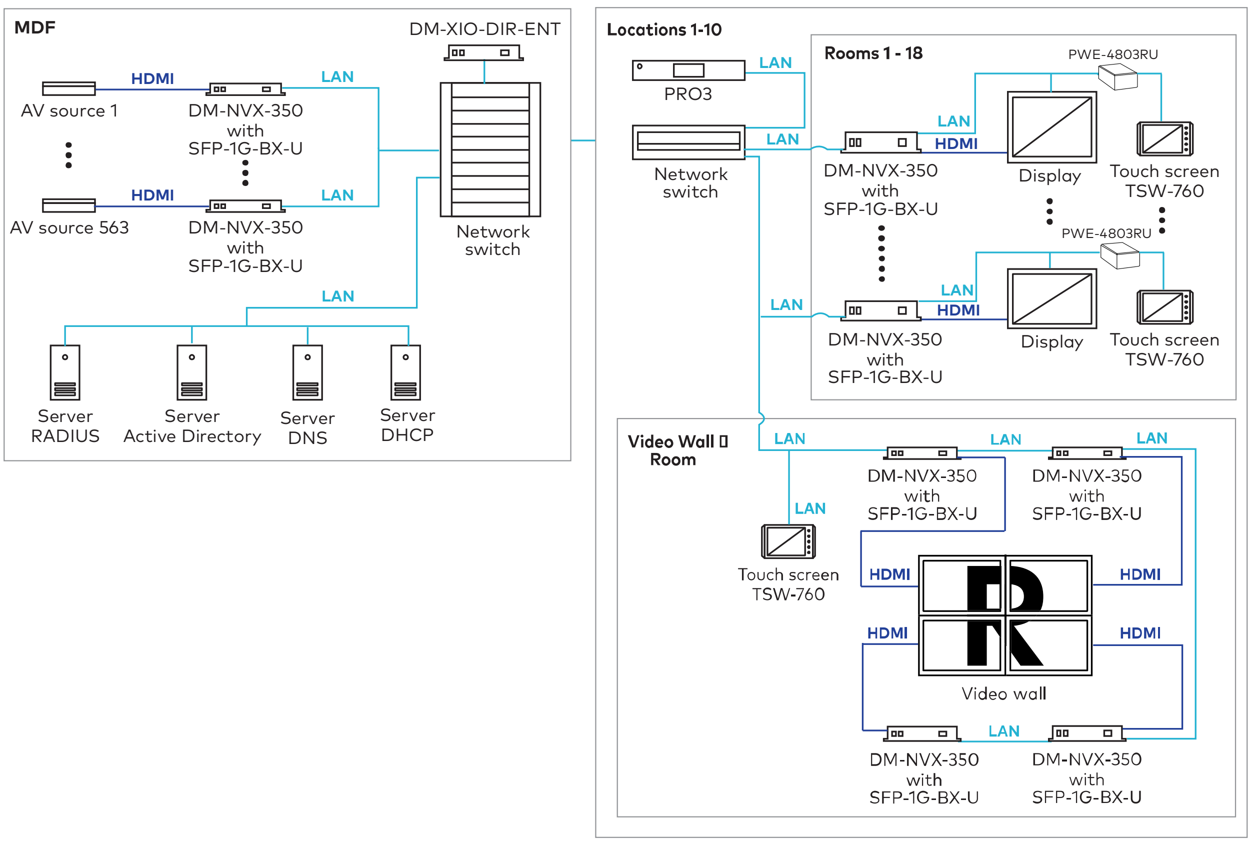
A client requires 4K AV distribution of 563 sources that are co-located at the MDF for 10 different locations on a campus up to 0.8 km (0.5 mi) from the MDF. Each location contains 18 separate displays and four 2 x 2 video walls across multiple rooms. The client needs to use a fiber-optic network for all video distribution. All device logins must be tied to the campus Active Directory, DHCP, and 802.1X services for policy reasons. Core redundancy is required to minimize campus-wide disruptions. Users must be able to switch between sources at any display independently.

Solution:

- The Crestron design is based on the use of DM-NVX-350 endpoints as encoders and decoders, a fiber-optic network across a large MDF, and the DM-XIO-DIR-ENT:
    - Endpoints consist of 563 DM-NVX-350 encoders at the MDF, 180 DM-NVX-350 decoders for the rooms, and 40 DM-NVX-350 decoders for the 2 x 2 video walls in the 10 locations (4 decoders for each location).
    - Single-mode 1310 nm/1490 nm fiber is used. The network switches are configured using SFP 1G BX downlink modules, and the DM-NVX-350 encoders and decoders use SFP-1G-BX-U uplink modules for fiber connections.
    - A DM-XIO-DIR-ENT allows fiber to be used for the DM NVX system. The DM-XIO-DIR-ENT is used to set up, control, and monitor the DM NVX system.
- A Crestron PRO3 control processor is used in each of the 10 locations.
- A TSW-760 touch screen is used in each of the 18 rooms across 10 locations, totaling 180 touch screens. In addition, a TSW-760 touch screen is used for each video wall room in the 10 locations, totaling 10 touch screens that provide user control of the entire system. Each touch screen is powered by a Crestron PWE-4803RU PoE injector.
- A tree architecture requires a minimum core switch bandwidth of 252 Gbps for 563 encoders and 252 (180 + 72) decoders. The existing core switch is capable of 1 Tbps and will be reused and reconfigured for 1 Tbps as required.
- Each of the 10 locations requires 22 DM-NVX-350 decoders to provide a nonblocking switch with at least 22 free ports.
- The network switches are configured to route the campus RADIUS server for 802.1X, the campus Active Directory server for login authentication at each endpoint, the campus DNS server for name assignment, and the campus DHCP server for IP assignment and MAC filtering; similarly, the endpoints are configured to utilize these services.

- Four of the 22 DM-NVX-350 decoders in each of the 10 locations are daisy chained to connect the decoders in the video wall rooms. The 3-port switch of the DM NVX endpoints consists of the following connections:
  - SFP-1G-BX-U connection to the edge switch
  - RJ-45 connection used in the daisy chain to connect the other video wall endpoints
  - RJ-45 connection to the TSW-760 touch screen for video wall room control

Case Study 3 Solution Diagram



Glossary

802.1P: A network quality of service labeling protocol that assigns a number from zero to seven to determine network traffic priority; defined in IEEE 802.1P-1998

802.1Q: A network protocol that allows for VLANs and tagging of VLAN traffic and enables 802.1P to provide quality of service features; defined in IEEE 802.1Q-2014

802.1X: A network control protocol to authenticate devices connected to an Ethernet network on a port-by-port basis by encapsulating the Extensible Authentication Protocol; defined in IEEE 802.1X-2010

Active Directory: An application protocol developed for Microsoft® Windows® networks that authenticates and authorizes users and devices using login mechanisms and also stores and controls additional information on the network regarding users and resources

Core: The central point of a network from which all network devices and intermediate infrastructure are normally accessible

Closet: The distribution point for networking infrastructure localized to a floor or group of rooms

Dynamic Host Configuration Protocol (DHCP): A network protocol that distributes network parameters such as IP addresses through a server to clients requesting them; defined in IETF RFC 2131

Domain Name System (DNS): A system of naming computers on a network that have numerical IP addresses; defined across multiple IETF RFCs starting with IETF RFC 1034

Domain Controller: A server-running domain service such as AD or LDAP

Extensible Authentication Protocol (EAP): A protocol for authentication of point-to-point network connections using multiple methods including TLS and MS-CHAP v2; defined in IETF RFC 3748 and IETF RFC 5247

Edge: The endpoint of a network connection that allows end device interconnection with the network

Extended Display Identification Data (EDID): A data structure usually communicated over HDMI and DVI interfaces between audio/video sources and displays to identify the capabilities of the devices on the link; defined in VESA EDID Version 3 and EIA/CEA-861

Intermediate Distribution Frame (IDF): The signal distribution frame that allows interconnection between the main distribution frame and premises closets

International Electrotechnical Commission (IEC): A nonprofit organization that publishes standards regarding electrical and electronic standards

Institute for Electrical and Electronics Engineers (IEEE): A nonprofit organization that publishes electrical and electronics standards particularly for network communication through the IEEE 802 family of standards

Internet Engineering Task Force **(IETF)**: A standards organization that establishes and maintains voluntary standards for Internet networking globally

Internet Group Management Protocol (IGMP): A network protocol that allows multicast traffic to pass over adjacent routers on an IPv4 network; defined in IETF RFC 2236 for v2, and IETF RFC 3376 and IETF RFC 4604 for v3

Internet Protocol (IP): A communications protocol that relays information across network boundaries between addresses; defined in IETF RFC 791 for IP version 4

Infrared (IR): A method of providing device control using light waves just beyond the range of red light

International Standardization Organization (ISO): A nongovernmental organization that publishes standards on all topics for international use, including audio and video compression standards; works jointly with the IEC to develop certain standards such as JPEG 2000

JPEG: An acronym for Joint Picture Experts Group

JPEG 2000: The image compression technology using wavelet-based scaling techniques to reduce image size without block noise and at high quality; defined in ISO/IEC 15444

Media Access Control (MAC): A 48-bit address in the Ethernet protocol that establishes the unique physical device in a network that is routed to or from that physical device

Main Distribution Frame (MDF): The signal distribution frame for networking that connects premises physical plant equipment to outside physical plant equipment

Moving Picture Experts Group (MPEG): A working group of the ISO and IEC that sets standards for audio and video compression and related technologies

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP): A network authentication protocol that is used for network devices by RADIUS servers. MS-CHAP is defined in IETF RFC 2433 for MS-CHAP v1 and IETF RFC 2759 for MS-CHAP v2.

Multicast: One-to-many data transfer that allows scalable distribution of audio and video in an efficient manner

Multi-Protocol Label Switching (MPLS): A labeling protocol for network traffic such that short labels rather than long network headers are used to route traffic appropriately; defined in IETF RFC 3031

Network Topology: The layout of a network as it would appear visually in a simplified form

Protocol Independent Multicast–Sparse Mode (PIM-SM): A protocol for routing multicast traffic such that the routes are optimized and effectively prevent flooding of uplinks in network infrastructure; defined in IETF RFC 7761

Plenum: Part of a building where heating, ventilation, and air conditioning are provided

Public Key Infrastructure (PKI): A set of procedures and policies for the different roles required in securely managing digital certificates and the infrastructure used to exchange both asymmetric encryption keys and symmetric encryption keys

Quality of Service (QoS): A performance improvement feature that prioritizes more important network traffic over less important traffic in a network switch

Remote Authentication Dial-in User Service (RADIUS): A network protocol that provides authentication, authorization, and accounting for network devices and users in a secure way, especially for IEEE 802. 1x protocol, and deployed in a client-server model; defined in IETF RFC 2865 and IETF RFC 2866

Request For Comments (RFC): A standards publication from the IETF

Real-time Transport Protocol (RTP): A network protocol for the actual delivery of audio and video streaming media; defined in IETF RFC 3550

Rapid Spanning Tree Protocol (RSTP): A network control protocol for discovering and accounting for network loops and redundancies; defined in IEEE 802. 1d-2004

Real-Time Streaming Protocol (RTSP): A network control protocol for streaming media to establish and control streaming audio and video sessions between endpoints; defined in IETF RFC 7826

Secure Shell (SSH): A protocol utilizing cryptography that secures network services such as a command line shell; defined across a number of IETF RFCs beginning with IETF RFC 4250 by the IETF SECSH working group

Structured Cabling: A standard for developing network and cable infrastructure; defined in TIA/EIA-568

Symmetric Encryption: An algorithm or method of using cryptography such that a single key is used for both the encryption and decryption of information to be protected

Transport Layer Security (TLS): A protocol implementing cryptographic security on a computer network; defined in IETF RFC 5246 and IETF RFC 6176

Transport Stream (TS): A media format that encapsulates audio, video, synchronization, and other information for transport; defined in ISO/IEC 13818-1

Universal Datagram Protocol (UDP): A protocol that transfers information over an IP network in a connectionless way such that data delivery is not guaranteed yet prevents the lack of a verified and established connection to prevent data delivery; defined in IETF RFC 768

Unicast: A one-to-one delivery protocol that is simple but not scalable for multipoint audio and video distribution

Virtual Local Area Network (VLAN): A nonphysically sequestered broadcast domain or partition isolated at the data link layer, effectively sequestering switch ports and network traffic across one or more switches from all other ports and traffic

This page is intentionally left blank.

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

Design Guide – DOC. 7977E
(2048398)
06.18
Specifications are subject to
change without notice.