DigitalMedia™ NVX Series System

Design Guide

Crestron Electronics, Inc.

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

Contents

Introduction

This document is provided as an aid to the design and installation of networked video and audio distribution systems using the Crestron® DM-NVX series line of products.

NVX is the world's first digital video distribution system capable of switching thousands of 4K video sources and displays at 60 frames per second with full 4:4:4 color sampling, High Dynamic Range (HDR), and low latency over long distances using flexible commodity Gigabit Ethernet fiber and copper network infrastructure.

With additional features for security, web-based configuration, local end-point video source switching, video wall, remote USB peripheral control, and analog audio source switching and playout, NVX is ideal for any application where scalability and flexibility with lower deployment cost per endpoint is required.

For additional details on functionality and configuration, refer to the DM-NVX Series Supplemental Guide (Doc. 7839) at www.crestron.com/manuals.

How NVX Works

Video distribution technology has evolved considerably since the emergence of analog video switching and amplification. Digital video carried over interfaces such as HDMI® technology has enabled high-quality experiences for average consumers. Despite this, inherent limitations from the perspective of scale, coverage distance, installation flexibility, and features persist because of the extreme high bandwidth imposed by uncompressed video interfaces such as HDMI and HDBaseT® technology, particularly at 4K resolutions. Yet the emergence of high-speed commodity network hardware and low-cost computing power has revolutionized long-distance, high-quality streaming video distribution on both private networks and the public Internet.

The cornerstone of NVX's ability to leverage Gigabit Ethernet infrastructure is the JPEG 2000 compression format. Unlike traditional JPEG or MPEG that breaks images down into blocks to remove visually redundant information, JPEG 2000 uses a method called wavelet-based compression. This type of compression, in conjunction with the high bit rates afforded by Gigabit Ethernet, recreates images with visually imperceptible losses in quality, even when compared to an uncompressed version of the original.

NVX can easily switch and move many video sources using Gigabit Ethernet infrastructure, resulting in considerable cost savings versus moving uncompressed lossless 4K 60 frames per second 4:4:4 video. More significantly, this bandwidth savings allows NVX to scale up the number of video sources and displays to much higher levels than is possible with uncompressed sources, with no additional latency (due to the close integration with the scaler during the decoding process).

NVX sends and receives video and audio by encapsulating it in an MPEG-2 Transport Stream (TS), then sending that transport stream using Real-time Transport Protocol (RTP) and Real-time Streaming Protocol (RTSP) over multicast Universal Datagram Protocol (UDP). This allows NVX to distribute video from one source to thousands of receivers on the network without resorting to inefficient unicast point-to-point links that would make high-quality, multipoint video distribution impossible.

Every NVX endpoint is dynamically configurable as either an output transmitter (encoder) or a receiver (decoder), using stand-alone endpoints as well as add-in cards in an NVX card chassis for denser aggregation of inputs and outputs.

NVX Design

Designing a network for NVX requires a concerted effort in gathering information and planning to implement correctly. This design guide assists the system designer in understanding the implications of NVX functionality on endpoints and the network. Throughout this process, ensure that the interaction between designer, installer, programmer, and end user is considered in all design decisions.

NVX Endpoint Design

The basic building block of an NVX system is the encoder and decoder endpoint. There are two primary types of endpoints available to the designer: stand-alone endpoints and chassis-based cards. Each endpoint is capable of operating as an encoder or as a decoder at a given time; specifically, one input or one output of an NVX endpoint is available as a TS/RTP/RTSP/UDP stream to and from one or more NVX endpoints.

Networking infrastructure is essential to NVX functionality, as all endpoints must connect to a purpose-designed nonblocking, multicast-enabled switched network in order to function correctly. The selection of appropriate network infrastructure components is essential to successful NVX implementations that can be reconfigured and maintained upon deployment.

NVX Endpoint Hardware Overview and Features

There are four models of DM® NVX hardware as follows:

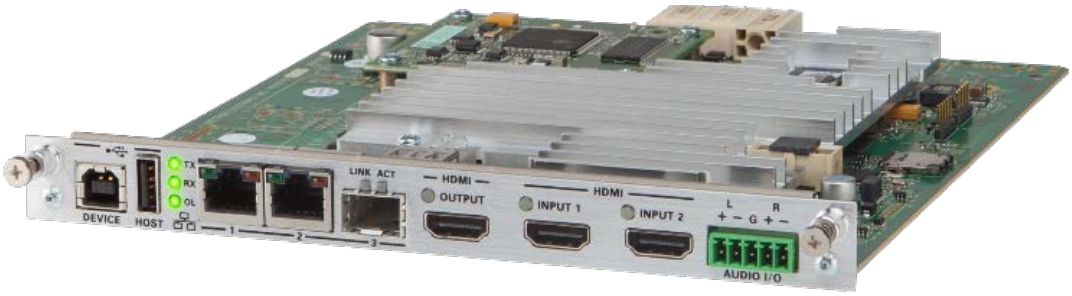
- The DM-NVX-350 and the DM-NVX-351 are stand-alone endpoints with IR and serial control, discrete device console connections via RJ45 and USB, and manual setup and reset buttons.
- The DM-NVX-350C and the DM-NVX-351C are card-based endpoints without IR and serial control that are used in conjunction with the DMF-CI-8 8-card chassis for sources in close proximity to a rack or for high endpoint density applications.

The DM-NVX-351 and DM-NVX-351C are also capable of downmixing a multichannel audio source carried over HDMI.

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



All endpoints, stand-alone or card-based, have the following physical connectivity:

- Two switchable local HDMI inputs for 4K 60fps 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, capable of local insertion of audio, replacement of HDMI source audio, or playout of audio
- Two RJ45 Gigabit Ethernet ports capable of 330 ft (100 m) distances over shielded Cat 5e/6/6a cable
- One SFP Gigabit Ethernet port for optional optical connection using Crestron SFP-1G transceiver modules
- One USB 2.0 host port for connecting a USB host, such as a PC
- One USB 2.0 device port for connecting keyboards, mice, and other peripherals

DM-NVX Hardware Model Differences

Product	Form Factor	Audio Downmix	Card Chassis Required	IR Out	Serial Out
DM-NVX-350	Stand-alone	No	No	Yes	Yes
DM-NVX-350C	Card	No	Yes	No	No
DM-NVX-351	Stand-alone	Yes	No	Yes	Yes
DM-NVX-351C	Card	Yes	Yes	No	No

Other key features available on all NVX hardware models include the following:

- Integrated Security: Every NVX endpoint integrates security features, including 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 can be passed between endpoints, allowing for easy control of source and display devices that support CEC.
- USB Routing: USB 2.0 may be routed from one NVX endpoint to another, independently of video and audio routing. One device must be configured as a USB host while the other device must be configured as a USB device port.
- 3D Surround Audio Support: Endpoints can pass through 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 is required for generating a stereo downmix if required.
- Secondary Audio: Encoders can generate a secondary audio stream that may be 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 RJ45 and one SFP module cage, enabling daisy chaining of endpoints and control of third-party devices in addition to primary NVX video stream I/O.
- Power-over-LAN: An RJ45 LAN port is provided with built-in Power-over-LAN power injection to provide power directly to an end device without an external power supply, and compatible with the DM-PSU-ULTRA-MIDSPAN.
- Video Wall: Up to 64 displays can be daisy chained across endpoints to provide multi-display video wall capability, with each endpoint providing fully customizable bezel compensation and zoom on any part of the source video.

For additional details on functionality and configuration, refer to the DM-NVX Series Supplemental Guide (Doc. 7839), the DM-NVX-350/DM-NVX-351 DO Guide (7799), and the DM-NVX-350C/DM-NVX-351C DO Guide (7975).

SFP-1G Modules

The SFP-1G family of modules are specifically designed for NVX to be able to enable additional gigabit network connectivity options for endpoints. While not technically required for endpoint functionality, SFP-1G modules enable fiber connectivity at much greater distances than traditional copper.

The available Crestron-certified SFP-1G modules include the following:

- SFP-1G-SX: 850 nm multimode fiber connections up to 1640 ft (550 m) over LC-terminated OM3 or OM4 fiber
- SFP-1G-LX: 1310 nm single-mode fiber connections up to 6.2 mi (10 km) using LC-terminated G.652 fiber
- SFP-1G-BX-U: 1310 nm/1490 nm single-mode fiber uplink connections up to 6.2 mi (10 km) using LC-terminated G.652 fiber
- SFP-1G-BX-D: 1310 nm/1490 nm single-mode fiber downlink connections up to 6.2mi (10 km) using LC-terminated G.652 fiber

SFP-1G Modules

For each endpoint, the connectivity options and distance requirements will determine the appropriate module to install.

XIO Director

Older pre-NVX digital video switch products did not make use of external network equipment in the video switching path, opting instead to handle such switching in a centralized card-based chassis and switch matrix. Due to the complexities of network video management, and to bridge the gap between traditional AV designers and more network-oriented AV designers and IT staff, XIO Director provides a comprehensive NVX configuration and signal routing tool.

Crestron XIO Director's web-based interface emulates a traditional hardware-based interface that allows users to automatically discover, configure, and route signals in an NVX network. XIO Director also offers domain grouping of individual subsystems, custom endpoint naming and search, XML-based device map file import and export for rapid configuration of multiple endpoints, along with logging, diagnostics, and SNMP messaging support for easy administration of NVX networks.

For additional information on XIO Director, please contact a Crestron sales representative.

Endpoint Bandwidth Design and Management

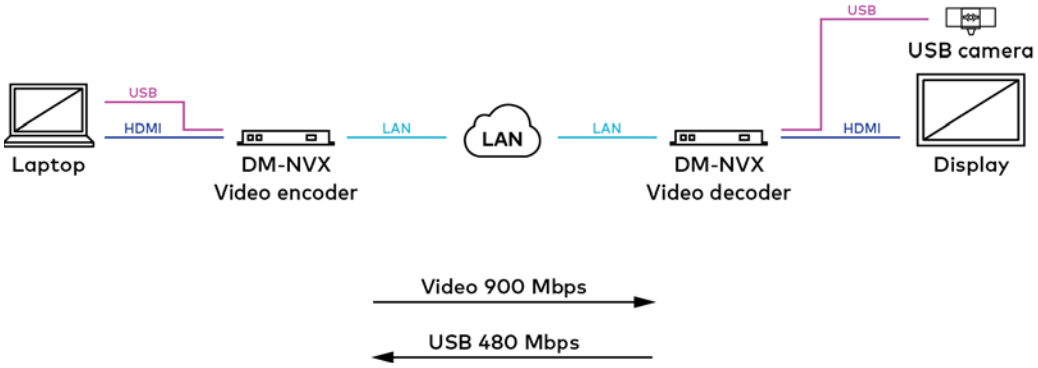
A single DM NVX network link can carry the following data streams:

- Primary Audio/Video stream: This is the video and audio from an HDMI input (or inserted via the audio line in the port) that is encoded and sent to the network for decoding by a remote endpoint.
- Secondary audio stream: Every encoder may generate a secondary audio stream that may be sent independently of the primary AV stream.
- USB device and host traffic: This is USB data from the NVX device or host port.
- Other Ethernet traffic: This traffic includes control data as well as data from NVX network ports connected to third-party devices such as displays or cameras, as well as network protocol traffic such as DHCP, DNS, or RADIUS for 802.1x.

The default settings should be sufficient for most installations. They may, be adjusted to accommodate unique situations. Since USB 2.0 can support up to 480 Mbps of traffic, this exceeds the default bandwidth reservations in the forward direction and may need to be adjusted for high-bandwidth devices. Devices such as keyboards and mice can consume anywhere between 0.1 Mbit/s sustained and 12 Mbit/s peak, whereas mass storage and web cameras can sustain up to 100 Mbit/s or more and peak at the USB 2.0 limit of 480 Mbit/s. It is recommended to contact the manufacturer of the USB device to confirm both the sustained and peak bandwidth of the device to be connected.

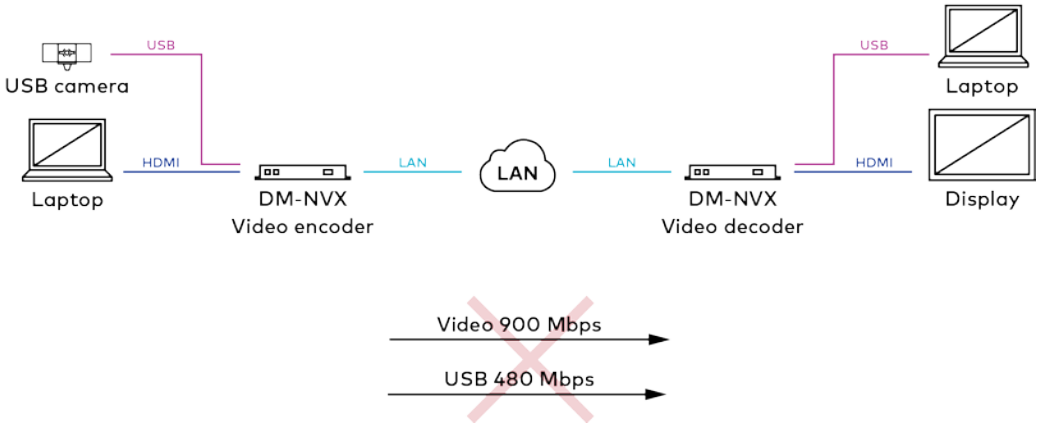
Ethernet bandwidth ratings are bidirectional, so full USB 2.0 bandwidth is supported in the reverse direction. Consider an NVX installation in which video from a PC is encoded and sent to a decoder at a display, and in which a high-bandwidth USB camera at the display is sending USB video back to the PC. While the sum of all traffic in this case may exceed a gigabit, the traffic in each direction is less than one gigabit and no bandwidth issues will exist.

Bidirectional Bandwidth under 1 Gbps Example



Conversely, an encoder that attempts to send 900 Mbps video and 480 Mbps USB 2.0 traffic will exceed the maximum network link bandwidth of 1 Gbps and fail.

Failed Link with Required Bandwidth Greater than 1 Gbps Example



For additional information on bandwidth management and configuration settings, refer to the DM-NVX Series Supplemental Guide (Doc. 7839).

Endpoint Design Considerations

With the basic tools for NVX endpoints available, the designer must carefully consider a number of factors for each endpoint to implement an optimal configuration for the installation. The design considerations include the following:

- If rack-mount sources are required or a high density of endpoints are in proximity to each other in distance, use DM-NVX-350C or DM-NVX-351C card versions of the endpoints instead of the DM-NVX-350 or DM-NVX-351 stand-alone endpoints.
- If simultaneous stereo downmix alongside multichannel audio output is required, use DM-NVX-351 or DM-NVX-351C instead of the DM-NVX-350 and DM-NVX-350C.

- Follow the guidelines for cable types as specified in TIA/EIA-568 for choosing and certifying cables in an NVX installation.

  The following table provides guidelines on some of the primary network connectivity options that may be used at the endpoint based on total distance.

  Primary Network Connectivity Guidelines

Distance / Connection	<100m	<550m	<10km
RJ45	Cat5e Cat6 Cat6a Cat 7	-	-
SFP-1G-SX	OM3 MMF OM4 MMF	OM3 MMF OM4 MMF	-
SFP-1G-LX	G.652 SMF	G.652 SMF	G.652 SMF
SFP-1G-BX-U	G.652 SMF	G.652 SMF	G.652 SMF
SFP-1G-BX-D	G.652 SMF	G.652 SMF	G.652 SMF

- The DM-NVX-350 and DM-NVX-351 provide IR and serial control ports to control in-room devices as a courtesy feature. Adding a Crestron control processor (such as a PRO3 or AV3) is a necessity in a design, however, if IR and serial ports are used anywhere in the design, or if relay I/O or Cresnet® device control is required.
- While both USB host and USB device ports are available on all NVX endpoints, only one of these ports is capable of use at a time. The USB port can instead be routed to a different endpoint than the video and be opposite in direction to the video traffic to maximize the use of the 1 Gbps link in both directions.
- Although typically USB ports are used for low-bandwidth devices such as keyboards and mice, high-bandwidth devices such as cameras and storage can have an impact on overall video bandwidth. For additional information on how to manage high-bandwidth USB devices and the direction of bandwidth consumption, refer to “Endpoint Bandwidth Design and Management” on page 5.
- If additional HDMI inputs are required for local switching at the endpoint within typical HDMI cable distances of 15 ft (5m), consider using other Crestron solutions in conjunction with the endpoint, such as the Crestron DM and DMPS families of products.
- If an endpoint will be dynamically reconfigurable as both an encoder and a decoder, it is critical to ensure that any external analog balanced audio connection is fixed in configuration and is not used for both input and output. Dependence on external device control via serial or IR ports on the endpoint should similarly be considered.
- In many NVX installations, a programmer must configure specific control surfaces and additional switch options at endpoints, such as Crestron touch screens and local HDMI switches, so be sure to consider such options from the beginning for first-time success.

NVX System Design

All NVX systems require an appropriately designed and provisioned Ethernet network to function correctly. Even smaller network implementations can require an experienced network designer depending on the overall project scope. Proactively gathering requirements and documentation, coordinating with customer IT staff, and completing network design prior to site work will result in efficiently designed and deployed NVX installations.

NVX System Design Overview

Design NVX networks to isolate network traffic on network segments specifically architected for NVX. This may be accomplished either physically using separate infrastructure or virtually using Virtual Local Area Network (VLANs) or Multi-Protocol Label Switching (MPLS). The primary role of NVX network segments is to carry NVX multicast streams as well as NVX control and ancillary traffic.

A secondary design decision must also be made as to where other Crestron network devices will be located relative to network infrastructure, and particularly whether such devices will coexist on the same segment as the NVX or another segment that has traversal capabilities (but not multicast enabled) to the NVX segment.

Other non-NVX networked AV devices may be placed on the NVX network segment so long as their bandwidth requirements are understood relative to the NVX endpoint bandwidth requirements.

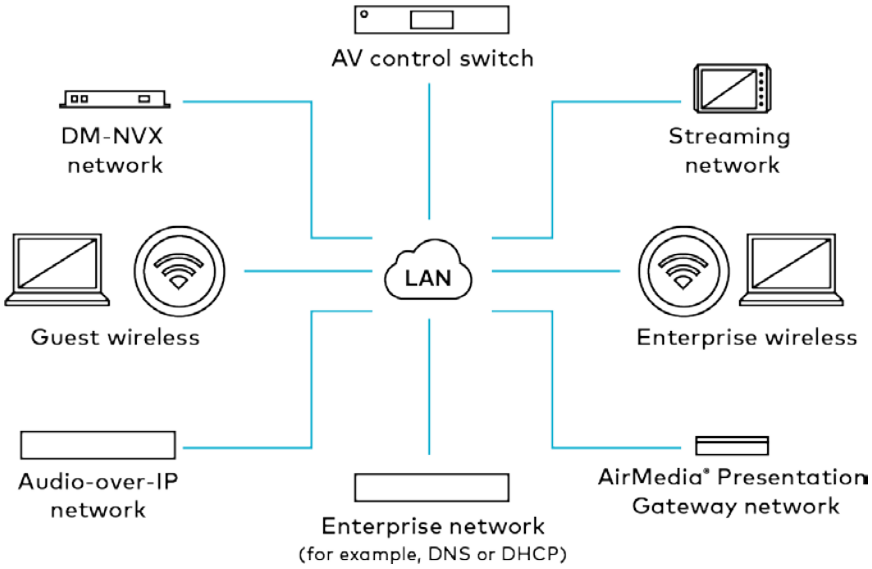
An NVX device can have up to three addresses.

- The first address is for control of the device as well as access to the web configuration interface and console.
- Two additional addresses are also required for multicast corresponding to the primary multicast stream of audio and video, and to the secondary multicast stream for secondary audio.

  Both multicast addresses must be set manually during endpoint configuration. It is therefore important to assign even-numbered IP addresses for the primary IP multicast stream since the secondary audio multicast stream address will be assigned a value of one higher than the primary IP multicast stream address by the endpoint.

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

Network Segmentation along Logical Boundaries



One of the key advantages to network video distribution is that any encoder may be routed to any decoder. For traditional circuit-switched systems such as HDBaseT, routes are limited by the size of the matrix switch. A properly designed and configured network can support thousands of endpoints with the ability to route any source to any destination.

The concept of a nonblocking architecture is the core design tenet that enables this flexibility. A nonblocking system has enough data bandwidth on all links to support all connected endpoints without any routing bottlenecks. Blocking must be considered at both the switch level and the network design level. NVX network switches must have enough switch fabric bandwidth to support full nonblocking bidirectional gigabit bandwidth on all ports simultaneously. While this is a common feature in most enterprise-grade gigabit network switches, it should not be assumed that a switch is nonblocking nor configured as such.

Most NVX installations require multiple network switches, due to either system size or physical layout. In these cases, NVX devices connect to Gigabit Ethernet ports, but switches are connected together with higher-bandwidth ports known as uplinks. It is strongly recommended that the bidirectional uplink bandwidth must be sufficient to handle traffic from all connected NVX devices. For network design purposes, assume that each NVX link consumes the full gigabit of link bandwidth.

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

Network Topologies

Devices such as NVX endpoints, control processors, touch screens, servers, personal computing devices and the like are connected directly to network switches. In a typical large network with multiple layers of switch hierarchy, these devices will be situated at the network's edge. The network edge switches are often (subsequently) connected via uplinks to other switches and routers to aggregate traffic from the network edge and form the network's core. The relationships between network switches and their interconnection to each other define the network's topology.

The NVX network designer must have a thorough understanding of network architecture and topology for a successful NVX deployment. The choice of topology, reuse of existing infrastructure and equipment, the number and specific needs of endpoints, and the level of redundancy will be the main drivers of network deployment cost and maintenance within the facility.

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

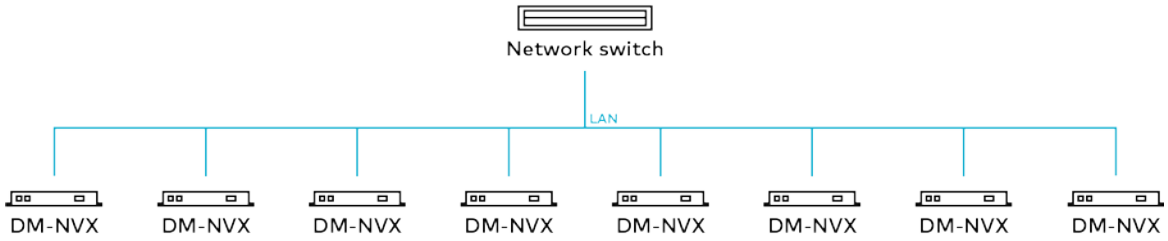
Star

The default recommended network topology is a star, which has a hub-and-spoke appearance that connects to the NVX endpoint and other devices through a single switch.

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

For small NVX systems that employ only one network switch, use a nonblocking switch so that there is no opportunity for a bottleneck. Star topologies can accommodate very large NVX installations by using large modular switch frames.

Star Network Using a Nonblocking Switch

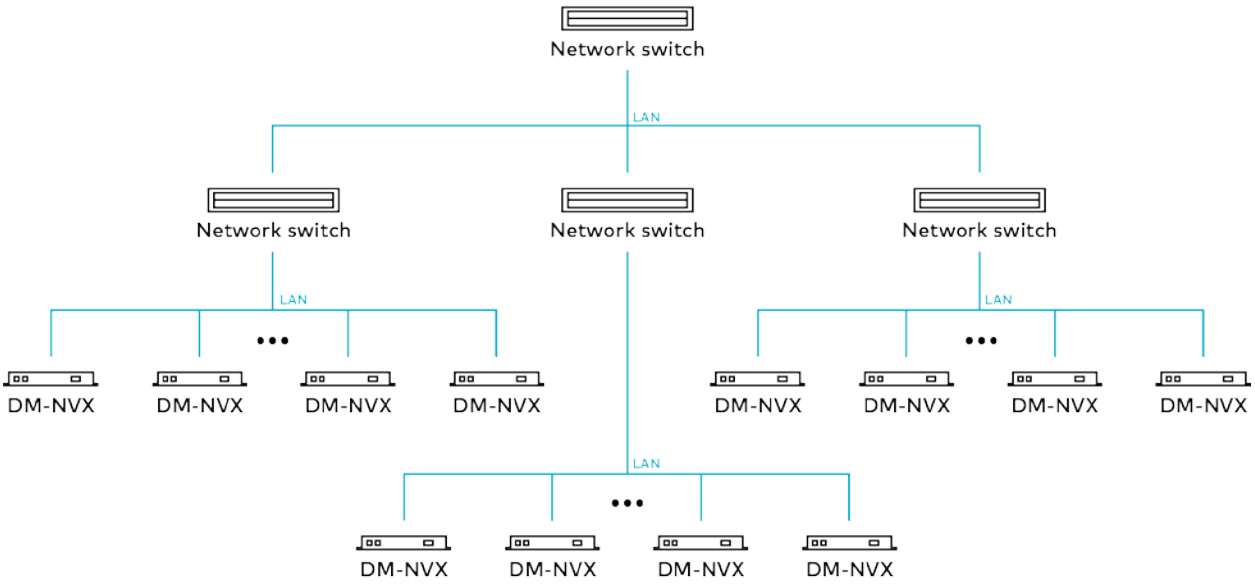


Tree

A tree network is a combination of more than one star network such that many stars exist on a core-switching infrastructure.

The tree network allows a failure in one part of the attached star networks without widely affecting the other star networks in turn. The core network denoted by the larger network switch can be configured for the purposes of redundancy and scalability as the network designer sees fit. This normally means the use of more than one switch per the network designer's requirements.

Tree Topology Using Nonblocking Switches on a Core Network



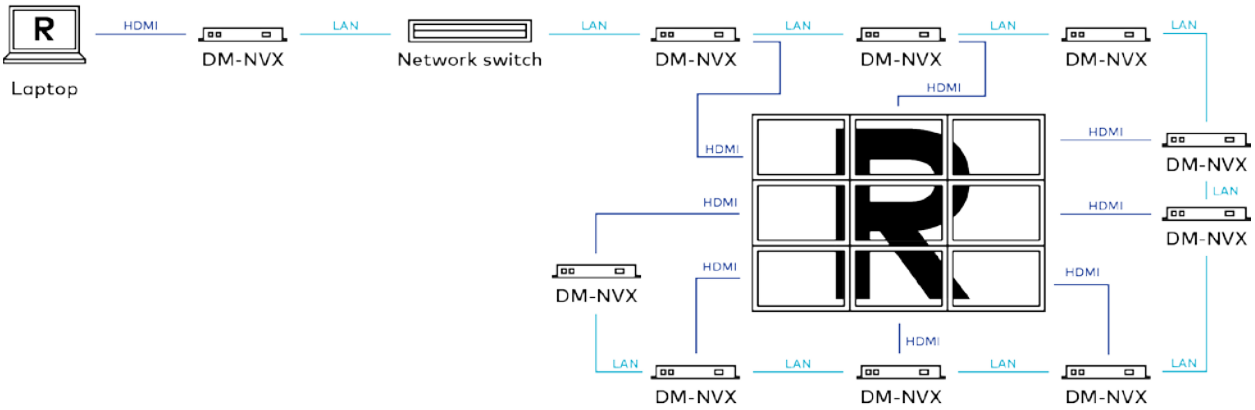
Daisy Chain

While not a topology per se, daisy chaining is a deployment methodology that NVX endpoints support which is appropriate only for specific deployment applications such as video walls or jury boxes where all displays receive the same video source as the first NVX in the chain.

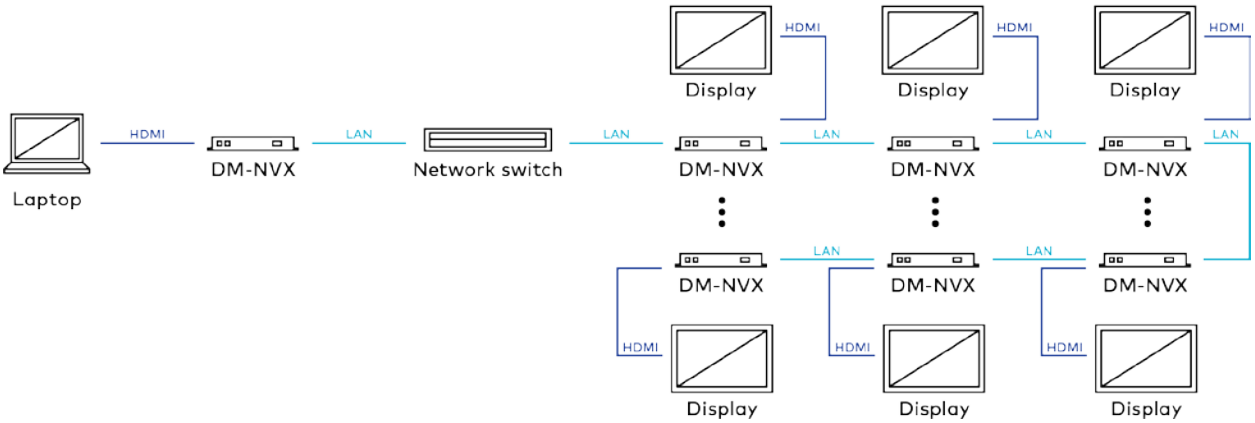
For video wall applications and any application where displays will be viewed near to each other and which share the same source, up to sixteen endpoints can be daisy chained together. Larger video walls should be divided on individual daisy chains no longer than sixteen endpoints.

For applications such as information, signage where more than one display will be readily viewable concurrently and not dependent on viewing of another display in the daisy chain, up to sixty-four endpoints can be daisy chained together.

Daisy Chain Network Configuration for 3x3 Video Wall



Daisy Chain Network Configuration for Twelve-Person Jury Box



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

Other Topologies and Network Functionality

There are other valid deployment topologies for NVX, such as ring and mesh. These deployments require project-specific discovery, engagement of the customer's IT staff, and advanced configuration of network switch beyond the scope of this guide.

For projects using advanced topologies for deployments, a networking professional with vendor-specific knowledge of the network hardware being deployed must be involved as early as possible in the network design process.

Network Multicast Functionality

NVX networks rely on multicast functionality exclusively to send and receive video, even in the simplest case of a single encoder endpoint and single decoder endpoint. Internet Group Management Protocol (IGMP) multicast in the Ethernet context replaces a fixed switching architecture in AV distribution. The challenge is to ensure that such traffic is capable of any permutation of one encoder to many decoders, and vice-versa without adversely affecting or being affected by other network devices.

Segregation of NVX traffic by using a VLAN or MPLS is generally the first step in enabling multicast. A VLAN or MPLS ensures that NVX traffic stays on the NVX network and does not route out to other network segments to interfere with their operation, nor allow traffic from other network segments to interfere with NVX operation. Within that segment, however, all ports can still be flooded by IGMP traffic regardless of if that traffic was intended to be sent or received by a network device at any given point in time. This will result in interference with the network operation and can even 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, a switch feature called IGMP snooping must be enabled, where snooping refers to the ability of the switch to limit multicast traffic only to ports between intended senders and receivers. There are different versions of IGMP snooping, but IGMP v3 is the currently supported version in NVX, with IGMP v2 support to follow in the near future.

In order for the switch to understand where route limiting will be specifically implemented in the network for multicast traffic, a network switch that assesses and maps the network for multicast nodes in the NVX network called an IGMP querier must be enabled. Normally, a single switch is selected by address to act as the IGMP querier, but the switch with the lowest numerical IP address on the network will typically be the default when multiple switches are configured as queriers. The default leave time for the querier (typically around 125s) is normally sufficient for an NVX network unless there are other specific requirements that a network designer must account for.

Further assisting the discovery and optimization of multicast network traffic routing is a feature called Protocol Independent Multicast (PIM). There are different modes of PIM such as Sparse Mode (PIM-SM), Dense Mode (PIM-DM) and Source-Specific (PIM-SSM), but NVX networks should be configured to use PIM-SM. PIM-SM assists in finding the shortest trees per path from any given multicast source to multicast receivers on a network and is more scalable than PIM-DM or PIM-SSM. PIM-SM also prevents edge-switch link saturation as well as network loops in the routing of multicast traffic.

Enabling network QoS is also useful in prioritizing NVX traffic over other ancillary traffic such as control traffic. Although there are multiple mechanisms that enable QoS, the most essential part of this is to enable the highest priority possible on IGMP multicast traffic. For example, enabling 802.1q VLAN tagging support in the switch, and then enabling and assigning an 802.1p priority (for example, 5, 6, or 7) to NVX addresses, ports or IGMP protocol traffic, will prioritize NVX traffic over other traffic at both the source and destination. Other traffic such as HTTP for web services, or SSH for console access, would be assigned lower priority numbers (for example, 0 to 4) based on their respective addresses, ports, or protocols. Other protocols exist for QoS (depending on the switch vendor) but are configured in a similar way to the 802.1p and 802.1q example. It is critical to ensure that all traffic types are affirmatively accounted for in QoS setup to ensure successful QoS operation.

Network Security

Security is an important consideration in all networks, including those built for NVX. Some of the security concerns network designers should be aware of includes the following:

- Unauthorized individuals attempting to eavesdrop on video, audio, or network traffic
- Individuals without proper authorization attempting to change specific settings, such as stream bandwidth, within endpoints and placing additional devices on the network
- Individuals attempting to commit acts of sabotage, such as bringing down a video network

From a design perspective, security requires the support of particular capabilities within all devices on the network. NVX employs the following security features:

- 802.1x is used to ensure that devices on the network have been explicitly sanctioned by the network administration team, which protects against unauthorized devices being added to the network and gaining access to sensitive content.
- Active Directory services for endpoint administration can be used to ensure that administrative privileges for NVX devices could be centrally managed, granted, and revoked when necessary.
- NVX endpoints use the industry-standard AES block cipher with robust PKI for stream encryption to protect content from unauthorized access as it traverses the network.
- SSL-based Secure Cresnet-over-IP (CIP) for NVX control ensures that control processors and NVX devices communicate with the intended party device and that commands and status cannot be monitored by any unauthorized device on the network.
- SSH-based command-line console access for device configuration and status protects the device console from access by unauthorized users.

Crestron's link encryption, Secure Crestron-over-IP, and SSH command line console access are both inherently available and automatically configured within devices and support software. The designer should therefore focus on 802.1x and Active Directory services within the design.

For additional information on deploying security with Crestron products, refer to the DM-NVX Series Supplemental Guide (Doc. 7839), the IP Considerations Guidelines for the IT Professional Design Guide (Doc. 4579), and the Crestron Secure Deployment Guide Online Help (OLH 5571).

Network Design Considerations

With the understanding of the main network implications of the NVX design, carefully 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. Employ sufficient switch bandwidth and port speeds, as 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 NVX endpoints and any additional needs.

- Choose an appropriate network topology. Consider all requirements for the network, including basic functionality and redundancy, and whether video walls or repetitive display signage are necessary. When planning on a topology for the network, ensure that existing network IT staff and experienced network architects are involved in these decisions.
- Enable an IGMP querier on at least one switch in the NVX network. The IGMP querier ensures that all switches know which multicast transmitters and receivers are connected to which switches in the network. Enabling IGMP querier on multiple switches causes the switch with the lowest value of IP source address to take precedence and act as the querier.
- Enable PIM-SM on all aggregation switches to ensure the multicast traffic does not flood out edge-switch uplinks.
- 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, preventing any potential denial of service or unauthorized traffic snooping and network analysis for weaknesses.
- Ensure VLANs or MPLS are implemented correctly. Leveraging existing switch infrastructure with VLANs or MPLS can cause conflicts with existing and future network provisioning needs. It also requires substantial network implementation and management experience to operate over the long term. If a dedicated network for NVX 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 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 one higher than the primary stream's IP address. For multicast IP address assignment, refer to the guidelines in IETF RFC 3171.
- Use Active Directory for administration security. The use of Active Directory with 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. NVX has the option to configure IP addresses of endpoints with both fixed IP addresses and by DHCP. However, using a DHCP server with short lease times, MAC address filtering, and sufficient address space for future needs makes network management easier.
- Enable IGMP v3 multicast snooping on all switches in the NVX network. This is a requirement for all designs to enable multicast delivery to multiple endpoints. Switches without IGMP snooping enabled that receive a multicast stream will transmit that stream to all ports simultaneously, immediately saturating all network links.
- Use RSTP on the network to ensure that network loops are discoverable and prevent deployment issues. Network management should account for RSTP discovery downtime upon network changes.
- Use and plan for XIO Director for endpoint management. XIO Director requires an additional network appliance whose inclusion in a design will require additional consideration to enable management of the entire NVX network from the XIO Director server.

- Use daisy chaining to connect video wall endpoints or repeated displays. In the case of 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 from device to device.
- Route and configure nondedicated DHCP, RADIUS, Active Directory, or other servers with NVX outside of the NVX network to have access to the NVX network appropriately to provide these services.
- Disable IGMP proxy on Crestron control processors with routers. Crestron control processors with routers, such as the CP3N, Pro3, AV3, and the DMPS3 line, should have IGMP proxy functionality disabled when connected to the NVX network to ensure NVX multicast traffic does not interfere with the control processor.
- Account for high-bandwidth external USB as an endpoint for bandwidth. If high-bandwidth USB devices are to be used, ensure that the bandwidth is accounted for as an entirely separate 1 Gbps link since USB 2.0 bandwidth can consume 480 Mbps of the 1 Gbps link.
- Leverage professionals with experience in high-performance network design, since most Pro AV designers are not typically expert network designers (and vice-versa). This can be of critical importance to the success of the network design from a both cost and schedule perspective.
- Ensure that multicast IP addresses do not share the multicast MAC addresses. Sharing of MAC addresses can cause network collisions and prevent the normal operation of the NVX network.

NVX System Installation

With a well-thought-out design of the NVX system in hand, the installer bridges the design and specification with real-world implementation. The challenges involved in NVX installation can be substantial yet manageable with sufficient forethought of some of the most common hazards that can prevent an optimal end user experience. As with the design phase, the installation phase should ensure that the interaction between designer, installer, programmer, and end user is considered in all installation decisions.

NVX Endpoint Installation

Each NVX endpoint will have unique installation requirements that depend on the following:

- If the network connectivity of the endpoint will be copper or fiber
- If the endpoint is card-based or stand-alone
- If the endpoint should be configured to encode or decode a stream, or will be switched dynamically between modes
- If there are additional local HDMI inputs to configure
- If source autoswitching or external switching control will be used
- If there are additional audio sources that require encoding
- If a USB device or host functionality is required
- If the endpoint is part of a video wall or goes to multiple identical displays

- If serial and/or IR control is required

For both types of endpoints, an external control surface such as a Crestron switch or touch panel may be linked through one of the spare LAN ports. The audio port may be repurposed to be a balanced line input for external analog audio input or for line output to an amplification and speaker system at the endpoint. The endpoint features and attached devices may 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 may be provided through Crestron HDMI breakout devices for tabletops and walls.

For stand-alone endpoints, the form factor of the endpoint is such that it can be mounted in any orientation as required with hardware. Typical locations for stand-alone endpoint mounting include inside drop ceilings, inside closets, underneath tables and in podiums.

The specific location is determined by several factors:

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

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

For card-based endpoints in a card chassis, the chassis is placed typically in a closet or locked rack near the source and display devices. Note again that serial and IR interfaces are not provided by card-based endpoints, so such functionality, when required, must be provided by other means, such as through a local Crestron control processor on the NVX network. To ensure that the environmental conditions in the rack are conditioned to meet the specifications outlined, refer to the DMF-CI-8 Supplemental Guide (Doc. 7861).

In order to ensure a first-time-right installation of the NVX endpoints, consider the following best practices:

- Plan the optimum location versus cabling for either the stand-alone endpoint or the card-based endpoint. Doing so can be critical to meeting the needs of the endpoint, especially when distance-limited HDMI cables are involved and cable infrastructure accommodation.
- Avoid end user direct access to the endpoint, because of the potential danger of end users inducing failures or creating a security risk due to unauthorized network access; ensure HDMI cables and wall plates are routed appropriately for user input away from the endpoint and that the endpoint is made as physically secure as possible.
- Use high quality certified HDMI cables in order to meet the minimum specifications for HDMI at 4K or even 1080 p and to prevent problems such as degradation or loss of video or audio caused by low-cost HDMI cables. Always use Category 2 certified HDMI cables such as the Crestron CBL-HD line available in lengths of up to 20 ft, or one of the Crestron HDMI powered cable extension solutions for special cases where more than 20 ft of cable is needed.

- Use properly terminated specification-compliant network cables. Network cabling needs to be either fiber of the correct wavelength, correctly terminated with a clean LC connector, or shielded copper Cat 5e, Cat 6, Cat 6a, or Cat 7 cable with an RJ45 connector, tested with an appropriate cable tester and compliant to TIA/EIA-568 cabling standards. Crestron DigitalMedia cable, connectors, and tools provide a solid foundation for such cabling.
- Observe cable minimum bend radiuses and pull forces, so as not to compromise cable integrity and cause intermittent or outright failures; careful planning along with proper installation techniques and tools ensure long-lasting reliable cable infrastructure.
- Use plenum-rated cables in plenum spaces. Cables such as Crestron DigitalMedia Plenum-rated cable are suitable, as is using fire-rated conduit for any fiber or copper cabling used in plenum spaces.
- Practice good cable dressing discipline to avoid and trace potential future issues. Cables connected to and from an endpoint can quickly become messy and difficult, especially for card-based endpoints in racks.
- Manage EDID and HDCP proactively. Although HDMI devices are capable of reading and interpreting EDID and HDCP automatically from sources and outputs alike, managing EDID and HDCP is often critical where specific output resolutions or endpoint capabilities are desired, particularly with HDR content only available using HDCP 2.2. For additional information, refer to the Crestron DigitalMedia System Design Guide (Doc. 4546).
- HDR and deep color sources may not display correctly on endpoints with non-HDR or non-deep color displays. Ensure that the capabilities of sources are matched to the capabilities of displays.
- Because endpoints can be difficult to find, which can lead to increased costs in programming and maintenance, use descriptive names for endpoints either through the NVX web configuration tool or by replacing the default name in the Crestron Toolbox™ console. 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 and compromising the installation. Ensure that all mounting points and mounting hardware for card chassis, cards, and stand-alone endpoints are used and secured.
- Leverage use of XIO Director for endpoint configuration. The presence of an XIO Director server makes it easy for an installer to configure and control multiple NVX endpoints on the network. Leverage whenever possible to assist in deployment of endpoints; coordinating with the network installers and network administrators to ensure access to XIO Director is essential to its timely use.
- Document everything during installation, and establish and publish drawings, lists, and descriptions for the installation of the endpoint. This can help those maintaining or upgrading the NVX network ensuring that they have everything they need in the future.

Follow these guidelines for a first-time-right maintenance-free installation and to reduce the time required to solve future support issues.

NVX Network Installation

The installation of an NVX network can vary greatly depending on a number of factors, including the following:

- Whether or not existing network infrastructure such as switches and cabling will be reused
- The location of closets, racks, IDFs, and the MDF/CDF relative to the endpoints

In practice, for most NVX network installation cases, at least some existing infrastructure will be used or repurposed for the installation.

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

- Use physical security for the network. All network locations, from MDF/CDF and IDF down to individual closets, should be physically secured from unauthorized access.
- Disable any unused ports on network switches, regardless of VLAN configuration, using the appropriate switch management software.
- Observe cable minimum bend radiuses and pull forces, so as not to compromise the cable integrity and cause intermittent or outright failures. Careful planning along with proper installation techniques and tools ensure a long-lasting reliable cable infrastructure.
- Use a structured cabling approach such as those described in the TIA/EIA-568 standard. Include but do not limit the use of keystones in jacks and patch panels, shielded solid copper conductor cable properly terminated into keystones for long permanent copper cable runs not exceeding 295 ft (90 m), premade stranded patch cables not exceeding 33 ft (10 m) to connect between patch panels. Use cable testers to verify the integrity of the installation, redundant capacity for future expansion and backup, and horizontal cabling strategies for runs to devices.
- Physically secure the endpoint to a fixed point or rack to prevent movement over time and compromising the installation. Ensure that all mounting points and mounting hardware for card chassis, cards, and stand-alone endpoints are used and secured.
- Use plenum-rated cables in plenum spaces. Cables such as Crestron DigitalMedia Plenum-rated cable are suitable, as is using fire-rated conduit for any fiber or copper cabling used in plenum spaces.
- Use Crestron switch configuration files, which configure many of the recommendations as a starting point by default, reducing deployment time.
- Configure routing of external supporting servers. If nondedicated DHCP, RADIUS, Active Directory, or other servers are to be used with NVX outside of the NVX network, ensure that these are routed, configured, and tested to have access to the NVX network appropriately to provide these services in the configuration specified by the network design.
- Ensure that all NVX network hardware and configurations are properly documented and accounted for (including spares) prior to network deployment.

Crestron Service Provider Handoff

Once the NVX network and endpoints installed and interconnected, Crestron Service Providers (CSPs) will often be needed. Typical activities of a CSP in an NVX installation can 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 like panels and switches
- Managing EDID for endpoint devices

It is critical for the installer to have sufficiently documented what was installed in the design, and to have any conflicts resolved that might exist in the design and/or installation, for the programmer to efficiently implement the end user functionality desired.

As CSPs implement and deploy the various portions of the program, installers and designers should test and review the functionality with the programmer to ensure that the design and installation goals have been met for end users. The best-planned designs and implementations can have problems even after final end user approval, so regular collaboration throughout the process is critically important.

Once final approval is granted, the programmer must document the program functionality so support staff for the NVX installation can address any future issues, and services and equipment be redeployed quickly and efficiently.

Case Studies

For reinforcement of the design and installation principles in this document, several case studies are provided below for additional context.

Case Study #1: Community College 4K AV Distribution via Network

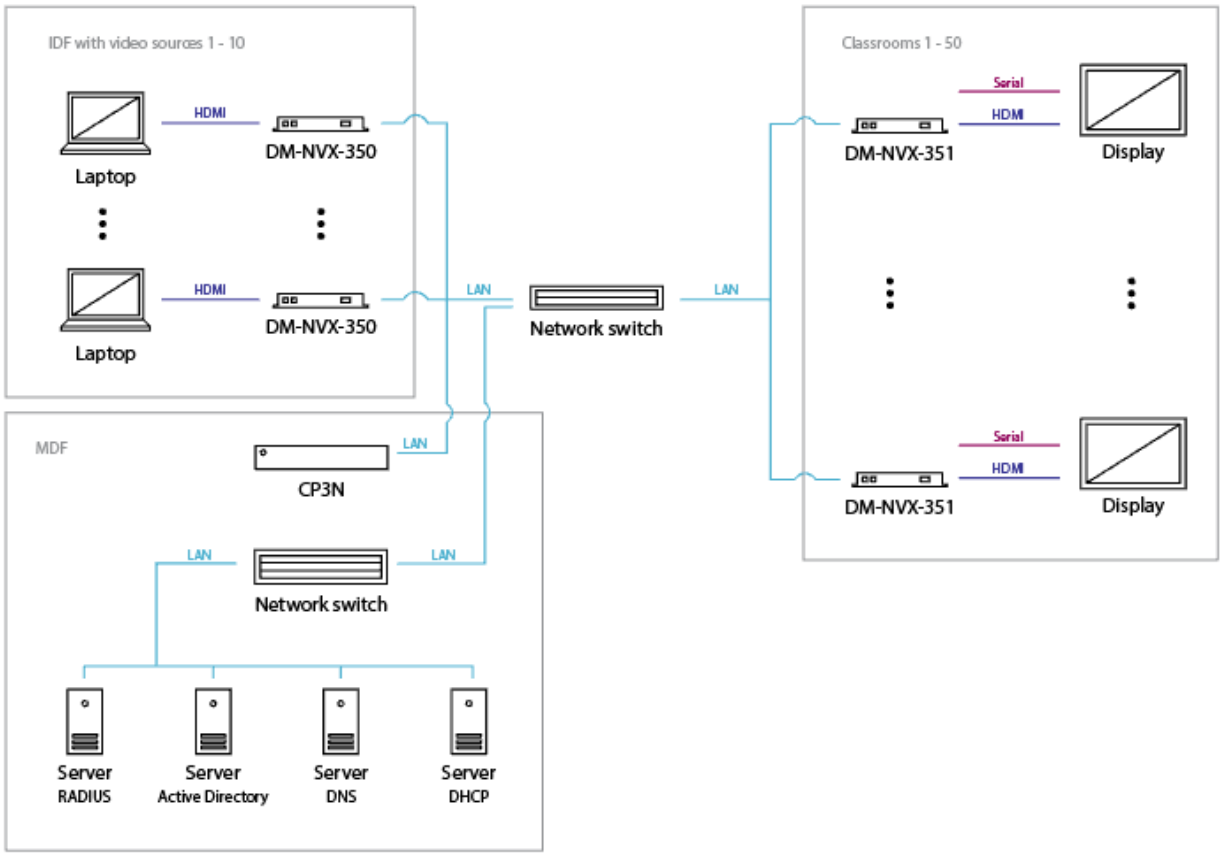
Problem:

A client wants to distribute ten 4K HDMI video sources located on the IDF Closet to fifty classrooms at a community college while maintaining the capability and flexibility of adding more classrooms and ten additional sources in the future. Use the existing network-cabling infrastructure while updating. Only the network hardware is a requirement. External sound bars must be used for audio output at the displays.

Solution:

- The Crestron design is based on 4K video distribution over a network.
- The system will include ten encoders at the IDF Closet with video source connections to that closet.
- The fifty rooms with displays will have a DM-NVX-350 decoder with no additional SFP-1G modules required. This is because there is no stereo audio downmix capability required and the density and distance of the application is not such that a card-based solution or optical network connectivity is required.
- The DM-NVX-350 at the displays locations will provide both video and control through serial control, so exclude DM-NVX-350C due to its lack of a serial port.
- Any source can be routed to any destination independently, so use a star network topology.
- The system can be controlled via Crestron Control App for mobile and tablet devices.
- Install a Crestron CP3N control processor at the IDF closet to provide centralized control for the entire system. Connect the processor to the network switch directly, as no additional external control from the control processor is necessary.
- Choose a nonblocking network switch with enough ports for ten video source endpoints, and fifty video display endpoints. The network can be reconfigured in the future to support an additional ten sources.

Case Study #1: Solution Diagram



Case Study #2: 4K Residential AV Distribution Network

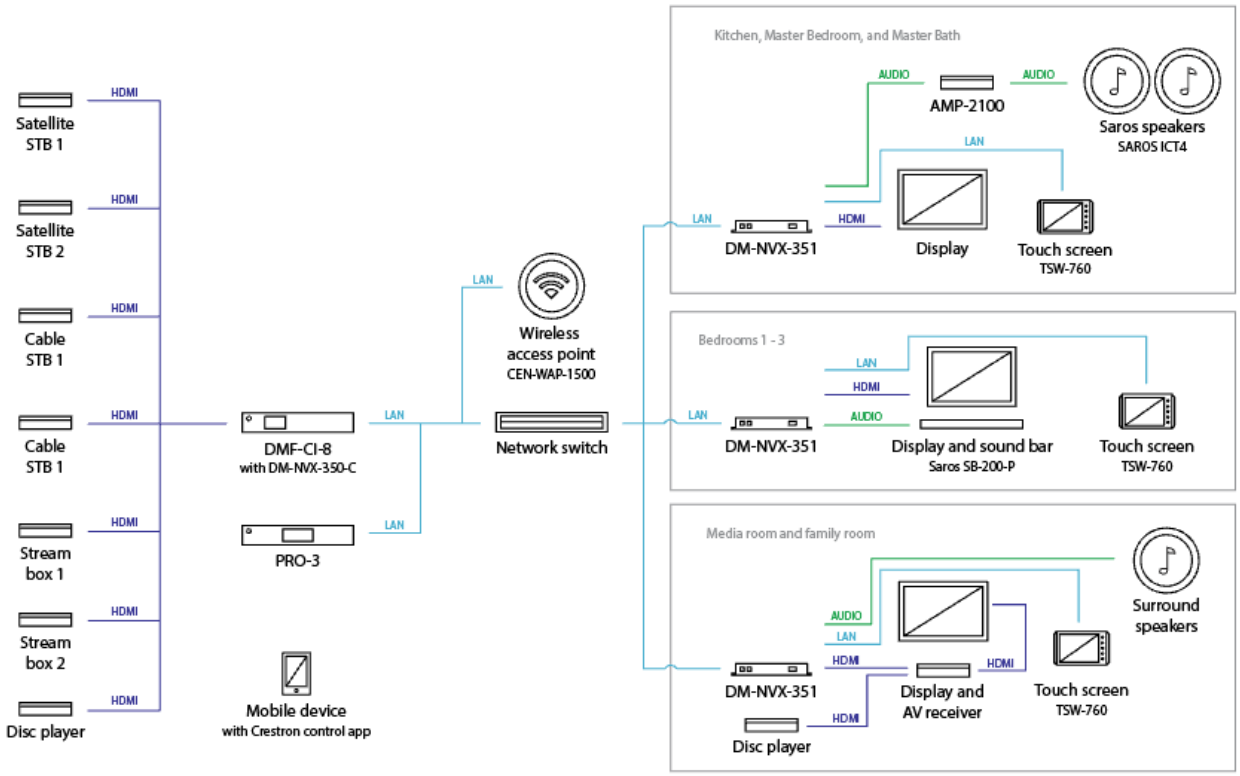
Problem:

A privately owned home needs a retrofit 4K video distribution system. Sources are in the basement rack room and are distributed to TV and Surround-Sound Receiver locations throughout the house. The system will include two cable set-top boxes, two satellite receivers, one Blu-ray player and two late-model Apple TV set-top boxes. The media room and family living room will have surround sound systems with a local 4K HDR Blu-ray player and 4K HDR displays. All other rooms will require external speakers with stereo output, with the kitchen, master bedroom and master bathroom requiring ceiling speakers. Touch screens are the desired control surfaces, with the media room and family living room not being able to have wire runs for these panels and only local power available. Existing network infrastructure can be reused.

Solution:

- Use a Crestron designed centralized 4K video distribution over an IP network.
- Locate the video distribution for the seven video sources at the basement rack. Connect all sources to seven DM-NVX-350C card endpoints installed in the DMF-CI-8 card cage rather than stand-alone endpoints due to density.
- The kitchen, master bedroom, and master bathroom will have DM-NVX-351's as decoders to provide both connection to the display and audio downmixing the DM-NVX-350 cannot provide. Connect a stereo line audio out to a two-channel amplifier with two Crestron Saros® IC4T 4 in ceiling speakers per room.
- Install a DM-NVX-351 decoder in bedrooms 1, 2, and 3 to provide display connection and audio downmixing. Connect the stereo line audio out will be connected to a Crestron Saros sound bar.
- The media room and family living room will include surround sound systems connected to DM-NVX-350 since downmix can now be performed by the surround sound system. The HDMI OUT from the surround sound system will connect to the display and in-room speakers connected to the surround sound system.
- Kitchen and bedrooms will use the TSW-760 touch screen as a control surface. They can also be controlled via Crestron Control App for mobile and tablet devices.
- Media room and family room will have TST-902 wireless touch screens for control (due to the cable routing constraint). They can also be controlled via Crestron Control App for mobile and tablet devices.
- Provide a Crestron PRO3 control processor with expansion cards to control the entire system and provide IR and other peripheral control.
- Any source can be routed to any destination independently, use a star network topology.
- A Crestron specified network switch will be required with enough ports for seven video source endpoints and five video display endpoints with future expansion for newer sources.

Case Study #2 Solution Diagram



Case Study #3: 4K AV Distribution over Fiber

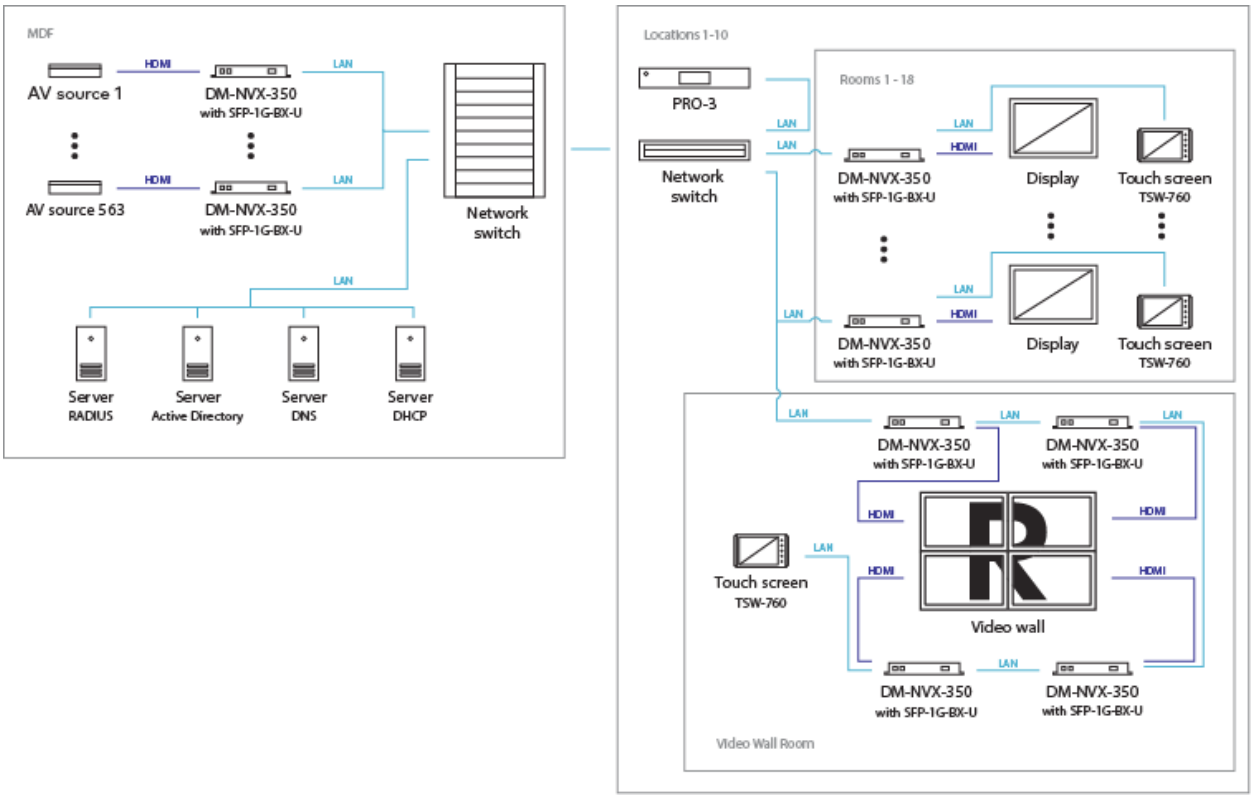
Problem:

A client requires AV distribution of 563 sources co-located at the MDF, for ten different locations on a campus up to 0.5 mi (0.8 km) from the MDF. Each location contains eighteen separate displays and four 2x2 video walls across multiple rooms. Client needs to use a fiber 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 but not endpoint redundancy is required to minimize campus-wide disruptions. All users should be able to switch between all sources at any display independently.

Solution:

- A centralized system was designed based on 4K video distribution over single-mode 1310 nm/1490 nm fiber coming to and from a large IDF.
- The system will use 563 DM-NVX-350 as encoder endpoints: 180 DM-NVX-350 decoder endpoints for the rooms, and 40 additional DM-NVX-350 decoder endpoints for the 2x2 video walls in each of the 10 locations. Neither density for cards nor stereo downmix is required for this application.
- Install ten Crestron PRO3 control processors, one in each location.
- Include180 TSW-760 touch panels for each of the eighteen rooms across ten locations, plus another ten TSW-760 touch panels for each video wall room in the ten locations; these panels provide user control of the entire system.
- All the DM-NVX-350 TX/RX will have SFP-1G-BX-U downlink modules for fiber connection, as the network switches will be configured with 1G BX downlink SFP modules; BX optical connections to and from NVX endpoints are denoted in blue in the diagram below.
- A tree architecture will imply a minimum core switch bandwidth of 252 Gbps, since there are 563 total encoders but 180+72 or 252 total decoders, but the existing core switch is capable of 1 Tbps and will be reused and configured as such.
- Each location requires 22 decoders, four of which will be daisy chained, to provide a nonblocking switch with at least 22 free ports.
- Configure the switches to route the campus RADIUS server for 802.1x, the campus DHCP server for IP assignment and MAC filtering, the campus DNS server for name assignment, and the campus Active Directory server for login authentication at each endpoint; similarly, configure the endpoints to utilize these services.
- Use a daisy chain to connect the endpoints in the video wall rooms. The use of the three ports illustrates why a 3-port switch is placed into the NVX endpoints: one for the SFP-1G-BX-U connection to the edge switch, one RJ45 used in the daisy chain to connect the other video wall endpoints, and the other RJ45 used to connect the TSW760 touch panel 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 that enables 802.1p to provide quality of service features; defined in IEEE 802.1q-2014

802.1x: A network access 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 (AD): An application protocol developed for Microsoft® Windows® networks that authenticates and authorizes users and devices using login mechanisms as well as storing and controlling 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 that is localized, usually 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 services such as Active Directory 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 to relay 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, with members throughout the world, 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 can be 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 for network devices that is used by RADIUS servers; defined in IETF RFC 2433 for MS-CHAP v1 and IETF RFC 2759 for MS-CHAP v2

Multicast: A 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 (PMI-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 that encrypt and validate digital information

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

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 for 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, as 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

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

Design Guide – DOC. 7977B
(2048398)
05.17