Networking Best Practice – White Paper

A guide to getting the most out of NDI® and your network.

This paper is intended to deliver the essential facts with best practices and is intended for professionals familiar with common networking devices and concepts. The wonderful thing about NDI® (Network Device Interface) is that it can be utilized on almost any Gigabit network. As production needs grow however, additional considerations will be required and that is what this paper will cover.

Overview

NDI is a royalty-free protocol developed by NewTek to enable video-compatible products to share video across a local area network (LAN). We believe that the future of the video industry is one in which video is transferred easily and efficiently via Internet Protocol (IP), and that this vision will largely supplant current industry-specific connection formats like HDMI, SDI, etc., in the production pipeline.

NDI allows multiple video systems to identify and communicate with one another over IP and to encode, transmit, and receive many streams of high-quality, low latency, frame-accurate video and audio in real time. NDI can benefit any network-connected video device, including video mixers, graphics systems, capture cards, and many other production devices.

NDI operates bi-directionally over a LAN with many video streams on a shared connection. Its encoding algorithm is resolution and frame-rate independent supporting 4K resolutions and beyond along with 16 channels and more of floating-point audio. The protocol also includes tools that implement video access rights, grouping, bi-directional metadata, and IP commands. NDI's superb performance over standard GigE networks makes it possible to transition facilities to an incredibly versatile IP video production pipeline without negating existing investments in SDI and HDMI cameras and infrastructure or costly new high-speed network infrastructures.

Discovery and Registration

Automatic Configuration

Sending and receiving video streams across an IP network requires applications that support video and are able to discover receiving applications that are looking for video. NDI resolves host names to IP addresses over the LAN and does so automatically. When you start an application that sends NDI, the devices that can receive NDI become

aware instantaneously. While this is a typical function on almost all networks, there are some cases where it is important to know how this works to properly configure networks utilizing managed data flows protocols.

As default, NDI utilizes mDNS (multicast Domain Name System)[1] to create the zero-configuration environment for discovery. This service sends an IP multicast message that asks the host to identify itself. The target machine then multicasts a message that includes its own IP address. This multicast is seen by all NDI receiving machines on the subnet, which then use the information in that message to update their own caches. These multicast queries are sent to a multicast address and thus, no single device is required to have global knowledge. When a service or device sees a query for any service it recognizes, it provides a DNS response with the information from its cache.

The primary benefits of using mDNS is that it requires little or no administration to set up. Unless the network is specifically configured to not allow mDNS, NDI sources will be discovered. This format works when no infrastructure is present and can span infrastructure failures.

The mDNS Ethernet frame is a multicast UDP packet that broadcasts to[2]:

- MAC address `01:00:5E:00:00:FB` (for IPv4)
- IPv4 address `224.0.0.251`
- UDP port `5353`

On Windows devices, choosing the network location type is critical for the successful discovery and registration of NDI. Typically, the first time a Windows machine is connected to a network, a dialog window appears that allows the user to choose the network location type: **Private** or **Public**. By default, Windows sets a new network location to **Public**. This location is designed to keep machines from being visible and responding to broadcast pings. This location type also affects mDNS responses and in turn, keeps NDI video streams from being discovered and registered on the network. For successful discovery and registration of NDI, network locations should be set to **Private**.

The **Domain** network location is used for domain networks, such as those at enterprise workplaces. This type of network location is controlled by the network administrator and cannot be selected or changed. In this type of configuration, mDNS discovery must be

[1] Apple's mDNS is published as a standards track proposal (RFC 6762) https://tools.ietf.org/html/rfc6762
[2] https://en.wikipedia.org/wiki/Multicast_DNS

allowed at the domain level. Because mDNS uses a link-local multicast address, its capacity is limited to a single physical or logical LAN.

Discovery Service

The NDI discovery service is designed to allow you to replace the automatic discovery NDI uses with a server that operates as a centralized registry of NDI sources.

This can be very helpful for installations where you wish to avoid having significant mDNS traffic for a large number of sources. It can also be useful in situation where multicast is not possible or desirable; it is very common for cloud computing services not to allow multicast traffic.

When using the discovery service, NDI can operate entirely in unicast mode and thus in almost any installation. The discovery server supports all NDI functionality including NDI groups.

Clients should be configured to connect with the discovery service instead of using mDNS to locate sources. When there is a discovery service, NDI applications will use both mDNS and the discovery server for finding and receiving to locate sources on the local network that are not on machines configured to use discovery.

For senders, if a discovery service is specified, then mDNS will not be used; these sources will only be visible to other finders and receivers that are configured to use the discovery server.

In order to configure the discovery service for NDI clients, you may use Access Manager (included in the NDI Tools bundle) to enter the IP address of the discovery server machine.

Within NDI version 5 there is full support for redundant NDI discovery servers. When one configures a discovery server it is possible to specify a comma delimited list of servers (e.g., “192.168.10.10, 192.168.10.12”) and then they will all be used simultaneously. If one of these servers then goes down, then as long as one remains active then all sources will always remain visible if at least one server remains active then no matter what the others do then all sources can be seen.

This multiple server capability can also be used to ensure entirely separate servers to allow sources to be broken into separate groups which can serve many workflows or security needs.

Once two NDI devices have discovered each other on the network, video can be passed from the sending device to the receiving device. After the compression of the

video, the NDI sending device opens a session to the receiving NDI device. At this point, we have two endpoints that consists of an IP address and a port number.

NDI Protocols

Reliable UDP
This is a new high-performance approach to transferring video and audio on a network. Real world testing has shown that in many problematic network configurations that performed poorly with previous versions of NDI and other video protocols now work perfectly with this version.

This uses a highly optimized UDP sender that supports very high latency connections (e.g., WAN or WiFi networks), with state-of-the-art congestion control and loss recovery (far superior to other reliable transfer protocols used in the industry), full inter-stream bandwidth management and connection sharing, no front of line queue blocking, reduced number of open ports and fully asynchronous sending and receiving.

Multipath TCP
This protocol permits transport across multiple NICs and all network paths, it is ensigned to use hardware-accelerated network adapters with adaptive bandwidth sharing across NICs.

Multipath TCP helps to maximize throughput, resource usage, and increase redundancy across the network, and is not disrupted by adding or dropping pathways and works across multiple network types such as wireless and mobile.

Single TCP
This is a network communications protocol, which enables two host systems to establish a connection and exchange data packets, and ensures data is delivered intact to the correct destination. TCP is typically grouped with IP (Internet Protocol) and known collectively as TCP/IP.

UDP with Forward Error Correction
This is an alternative protocol to TCP that is used when reliable delivery of data packets in not required. UDP is typically used for applications where timeliness is of higher priority than accuracy, such as streaming media, teleconferencing, and voice-over-IP (VoIP). Forward error correction (FEC) is a method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver)

NDI Related Network Ports

Port number	Type	Use
5353	UDP	This is the standard port used for mDNS communication and is always used for multicast sending of the current sources onto the network.
5959	TCP	NDI Discovery Server is an optional method to have NDI devices perform discovery. This can be beneficial in large configurations, when you need to connect NDI devices between subnets or if mDNS is blocked.
5960	TCP	This is a TCP port used for remote sources to query this machine and discover all of the sources running on it. This is used for instance when a machine is added by an IP address in the access manager so that from an IP address alone all of the sources currently running on that machine can be discovered automatically.
5961 and up	TCP	These are the base TCP connections used for each NDI stream. For each current connection, at least one port number will be used in this range.
5960 and up	UDP	In version 5 and above, when using reliable UDP connections it will use a very small number of ports in the range of 5960 for UDP. These port numbers are shared with the TCP connections. Because connection sharing is used in this mode, the number of ports required is very limited and only one port is needed per NDI process running and not one port per NDI connection.
6960 and up	TCP/UDP	When using multi-TCP or UDP receiving, at least one port number in this range will be used for each connection.
7960 and up	TCP/UDP	When using multi-TCP, unicast UDP, or multicast UDP sending, at least one port number in this range will be used for each connection.
Ephemeral	TCP	Legacy to NDI v1 - The current versions (4.6 and later) no longer use any ports in the ephemeral port range.

Getting video across the network

Video, just like voice data in VoIP systems, is a very demanding data stream and will immediately expose a weakness in a network. The network must support multiple video, audio, and data streams in a reliable, synchronized manner without disruption. When delay, packet

loss, and jitter reach thresholds where the video is impacted visually, the usefulness of that video drops to zero. It is important to understand the complexities of video in IP data networks so that these factors can be mitigated.

Networks that are designed to move NDI video streams should be thought of as being primarily utilized for video. IP networks are by their very nature “best effort delivery” systems and were originally developed for the transport of data. Data services, by contrast to video, can function happily with packet retransmissions, lost packets, and even packets arriving out of order. Video streams, while still data, are much more rigid in their requirements. With the use of modern networking equipment and proper configuration, video can move across networks whilst still obtaining low latency, frame accuracy, and high-quality requirements necessary for live video production.

Network Layout

NDI is designed for use with standard consumer off-the-shelf (COTS) networking devices. Looking closely at the network topology and configuration will help to ensure the maximum possible bandwidth is available.

When selecting a network switch, it is important to check the throughput speeds. Ensure that each port is full duplex (i.e., bi-directional communication) and that the upstream and downstream data speeds for each port are at least 1 Gigabit per second (Gbps). It is best to force the ports on managed switches to utilize 1 Gbps in contrast with Auto Negotiation. The use of Auto Negotiation can sometimes result in 100Mb connections or even lower, which does not renegotiate until the port is flooded with traffic for some time. Also, poor termination of RJ-45 connectors can impact Auto Negotiation.

When considering network switches that include 10 Gigabit per second ports, the same suggestion applies. Many switches manufactured at the time of writing may share bandwidth across the backplane of multiple ports. Since these ports are generally reserved for linking to other switches, the specification for throughput may be listed differently than the Gigabit port section in the product documentation.

When possible, it is best to use switches from the same manufacturer, or ideally, the same model of switch, throughout a single subnet. This will simplify configuration and lessen the chances of compatibility and configuration issues.

Bandwidth

NDI operates most efficiently in a dedicated network with high bandwidth and high availability. This contrasts with unmanaged environments such as the public Internet or networks where video rides along with data without priority.

Gigabit (1000 Mbps) networks are essential in production workflows. A typical NDI stream consisting of 1080 60P video yields a data rate up to 150 Mbps per stream. This extremely efficient stream is designed to have very low latency and allows multiple streams to be stacked

together on a single Gigabit network. Even so, it may be that a production environment will require more capacity based on simultaneous number of NDI streams required.

The following table is intended as a guide for calculating bandwidth needs based on video resolutions and frame rates. It should be noted however that NDI is not deterministic. Bandwidth needed for NDI should be based on determination of the average utilization required[3].

NDI High Bandwidth

Resolution/Framerate	Maximum Bandwidth Mbit/Sec	Maximum Bandwidth w/ Alpha Mbit/Sec	Proxy (no Aplha support)
1920*1080 50i	105	128	640*360 - 30Mbit/s
1920*1080 60i	112	140	640*360 - 30Mbit/s
1920*1080 50P	125	156	640*360 - 30Mbit/s
1920*1080 60P	132	165	640*360 - 30Mbit/s
3840*2160 50i	158	197	640*360 - 30Mbit/s
3840*2160 60i	171	214	640*360 - 30Mbit/s
3840*2160 50P	223	279	640*360 - 30Mbit/s
3840*2160 60P	249	312	640*360 - 30Mbit/s

NDI|HX H.264 & HEVC

	NDI|HX H.264	NDI|HX HEVC
Resolution/Framerate	Maximum Bandwidth Mbit/Sec	Maximum Bandwidth Mbit/Sec
1920*1080 50i	9.6	6.7
1920*1080 60i	10.5	7.4
1920*1080 50P	14.2	9.8
1920*1080 60P	15.9	10.9
3840*2160 50i	19.1	13.2
3840*2160 60i	20.6	14.3

[3] Bandwidth numbers are given as reference and are subject to change

3840*2160 50P	26.8	18.7
3840*2160 60P	30	21

Network Interface Settings

NDI is designed to enable successful video transport using the default configurations of network interface drivers, however most recent network interface drivers do support configuration of advanced properties that can help optimize NDI transmission.

Consider the following adjustments but note that adjusting on individual adapters can significantly affect performance and reliability; both positively and negatively. It is important to consider testing performance with a network analyzer before and after each setting change. The following adjustments are intended to help; however, performance will depend on network and usage (names and available settings vary between vendors, adapter models, and even between different driver versions):

Speed and Duplex: This setting allows for selection of the desired speed and duplex of the network adapter. Usually this is set to Auto Negotiation. To ensure the maximum available throughput, this setting should be set to 1 Gbps Full Duplex or higher if supported.

Energy Efficient Ethernet: When enabled, this allows the adapter to engage power saving features while keeping connections active. This technology uses the standard IEEE 802.3az to allow for less power during periods of low data activity. Adapters that utilize the IEEE 802.3az standard should have no impact on performance of NDI, however some integrated circuits exist that were developed before the standard was finalized or do not adhere to the standard at all. In these cases, it is best to disable the energy efficiency while determining best network optimization.

NIC Selection

Starting in NDI version 5, this lists all the network adapters that will be used for network transmission.

One or more NICs can be used for transmission and receipt of video and audio data. This capability can be used to ensure that the NDI primary stream data remains on a particular group of network adapters, for instance allowing you to ensure that dedicated audio is on a separate network card from the NDI video. It is generally preferred that you let NDI select the network adapters automatically which can smartly select which to use and how to choose the ones that result in the best bandwidth. While in some modes NDI can automatically balance bandwidth across multiple NICs, it is normally better for you to use NIC teaming at a machine configuration level which can result in much better performance than what is possible in software. If this setting is configured incorrectly to specify NICs that might not exist, then NDI might fail to function correctly. Also please note that the operation of computer systems that are separately on entirely different networks with different IP address ranges is often not handled robustly by the operating system and NDI might not fully function in these configurations.

NIC Selection configuration is part of NDI Access Manager.

Encoding and Decoding

Compression

NDI uses compression to enable transmission of many video streams across existing infrastructure, specifically discrete cosine transform (DCT), which converts video signals into elementary frequency components. This method of compression is commonly used in encoding formats and mezzanine codecs within the industry.

One of the most efficient codecs in existence, NDI achieves significantly better compression than many codecs that have been accepted for professional broadcast use. On a typical, modern Intel-based i7 processor, the codec can compress a video stream to following benchmarks:

The peak signal-to-noise ratio (PSNR) of the NDI codec exceeds 70dB for typical video content. Uniquely, and importantly, NDI is the first ever codec to provide multi-generational stability. This means that once a video signal is compressed, there is no further loss. As a practical example, generation 2 and generation 1000 of a decode-to-encode sequence would be identical.

The NDI codec is designed to run very fast and is largely implemented in hand-written assembly to ensure that the process of compressing video frames occurs as quickly as possible. Latency is both a factor of the network connection and the endpoint products. NDI has a technical latency of 16 video scan lines, although in practice, most implementations would be one field of latency. Hardware implementations can provide full end-to-end latency of within 8 scan lines.

NDI|HX

NDI is available in some devices and applications using a different compression codec than high bandwidth NDI. This variation is known as NDI|HX, which stands for NDI 'High Efficiency'. Devices that using this version of NDI will be labeled with the HX moniker. HX offers for similar video quality at a much lower bit rate, which can be useful in situations where bandwidth is limited, like Fast Ethernet networks, WiFi or WAN connections.

NDI|HX is commonly found in hardware devices, like PTZ cameras and mobile phones, but it is possible to have HX in software applications as well. Software applications using NDI|HX will leverage the GPU on the computer for enhanced encoding performance. For this reason, having a good GPU on the system is an advantage.

There are two variations of NDI|HX. NDI|HX v1 which requires the use of an 'HX Driver' which is included with NDI Tools and NDI|HX v2 which can directly connect with NDI applications. NDI|HX v1 is no longer used for new product development, new NDI|HX products released into the market will use NDI|HX v2.

NDI 5 remote connections use NDI|HX for transmission of signals over the Internet.

Formats

NDI supports multicast-based video sources using multicast UDP with forwards error correction to insure against packet loss. Multicasting allows for a single NDI source to be delivered to multiple receivers by replicating the NDI packets from the sender to any number of receivers. It is important to be aware that using multicast on a network that is not properly configured can produce undesirable results and cripple network performance. For this reason, multicast sending is disabled by default.

For successful multicasting, the use of Internet Group Management Protocol (IGMP) is encouraged. IGMP allows the receiving NDI systems to request access to the sender. Without IGMP querying and snooping, Multicast traffic is treated the same as broadcast transmission resulting in packet forwarding to all ports on the network. With IGMP snooping, multicast NDI traffic is forwarded only to the receivers that subscribe to the multicast NDI stream.

NDI subscribes to a multicast group and will unsubscribe when that stream is no longer needed. The management of multicast subscriptions is handled by a routing querier on the network.

While video and audio data are delivered to the network via multicast delivery, each receiver also connects to the sender via a unicast TCP connection for bi-directional communication of metadata (e.g., PTZ control, tally, etc.)

NDI in Cloud

Setting up an NDI-based video production in a Virtual Private Cloud is quite easy; the first step is to define how to make NDI Discovery and Registration working in a VPC. Cloud providers allow to create a multicast domain, multicast is required to use mDNS-based discovery and registration. This setup requires to create a transit gateway with multicast enabled. Enabling multicast in cloud might require specific knowledge, for this reason the easiest solution to enable the NDI Discovery and registration is to setup a Discovery Service. To run NDI Discovery Service just requires a basic Windows or Linux-based instance.

Summary

This paper does not aim to cover or deliver a blueprint for every permutation of every production workflow or network set-up out there – but rather to equip professionals with the information needed to get the best performance out of most environments. Network professionals curate the instrument that makes NDI sing, and we hope you will find the information enclosed of use in your task.

For the very latest news and information on NDI, visit NDI.tv

Glossary

Cache
Cache refers to a reserved section of computer memory or an independent high-speed storage device used to accelerate access and retrieval of commonly used data.

Domain
A domain refers to a LAN subnetwork of users, systems, devices, and servers. Domain can also refer to the IP address of a website on the Internet.

DNS
DNS (Doman Name System) is a system used by the Internet and private networks to translate domain names into IP addresses.

mDNS
mDNS (multicast DNS) refers to the use of IP multicast with DNS to translate domain names into IP addresses and provide service discovery in a network that does not have access to a DNS server.

Ethernet
Ethernet, standardized as IEEE 802.3, refers to a series of LAN (Local Area Network) technologies used to connect computers and other devices to a home or business network. Ethernet is a physical and data link layer networking protocol that supports data transfer rates starting at 10 Mbps, typically over twisted pair cabling, but also fiber optic and coaxial cabling.

IGMP
IGMP (Internet Group Management Protocol) is the protocol used in IP multicasting that allows a host to report its multicast group membership to networked routers in order to receive data, messages, or content addressed to the designated multicast group.

IP
IP (Internet Protocol) is the communications protocol for the Internet, many wide area networks (WANs) and most local area networks (LANs) that define the rules, formats, and address scheme for exchanging datagrams or packets between a source computer or device and a destination computer or device.

IPv4
IPv4 (Internet Protocol Version 4) is the fourth and most commonly used version of the Internet Protocol. IPv4 uses a 32-bit IP address scheme for network identification and communication, with each unique IP address expressed as four numbers (between 0 and 255) separated by decimal points.

IPv6
IPv6 (Internet Protocol version 6) is the latest version of the Internet Protocol, developed to eventually replace IPv4 (Internet Protocol version 4). IPv6 uses a 128-bit IP address scheme for network identification and communication, with each unique IP address expressed as eight groups of four hexadecimal digits (numbers from 0-9 or letters from A-F) separated by colons. In

addition to increasing the number of available IP addresses exponentially, IPv6 simplifies and streamlines network communication, while increasing security, compatibility, and efficiency.

LAN

LAN (Local Area Network) is a network that connects computers and devices in a room, building or group of buildings. LANs are typically deployed in homes, offices, and schools, where users share access to the same server, resources, and data storage. A system of LANs can also be connected to form a WAN (Wide Area Network).

Layer 2

Layer 2 refers to the second layer, or Data Link layer, of the OSI networking model. A layer 2 switch uses hardware-based switching to transmit data between connected devices based on their MAC (Media Access Control) layer addresses.

Layer 3

Layer 3 refers to the third layer, or Network layer, of the OSI networking model. A layer 3 switch uses hardware-based switching to transmit data between connected devices based on their IP (Internet Protocol) addresses. A layer 3 switch can support packet inspection and routing protocols to prioritize and forward traffic.

MAC Address

MAC (Media Access Control) address refers to a unique physical address that identifies a network node.

Mbps

Mbps (Megabits per second) is a unit of measurement for data transfer speed, with one megabit equal to one million bits. Network transmission are commonly measured in Mbps.

NDI

NDI (Network Device Interface) is an open protocol developed by NewTek for IP transmission and live production using standard LAN networking. NDI allows networked video systems to identify and communicate with each other over IP, and encode, transmit and receive multiple streams of broadcast-quality, low-latency, frame-accurate video and audio in real time.

OSI

The OSI (Open System Interconnection) reference model is a standard that defines worldwide network communication, developed by ISO (International Organization for Standardization). The OSI reference model divides network communication into seven layers: 1) Physical, 2) Data Link, 3) Network, 4) Transport, 5) Session, 6) Presentation, and 7) Application.

Packet (Frame)

A packet, also known as a frame or datagram, is a unit of data transmitted over a packet-switched network, such as a LAN, WAN, or the Internet.

Port

A port is a communications channel for data transmission to and from a computer on a network. Each port is identified by a 16-bit number between 0 and 65535, with each process, application or service using a specific port, or multiple ports, for data transmission. Port can also refer to a

hardware socket used to physically connect a device or device cable to your computer or network.

QoS
Qos (Quality of Service) is the measure of performance for system or network, with considerations that include availability, bandwidth, latency, and reliability. QoS can also refer to the prioritization of network traffic to ensure a minimum or required level of service, predictability, and/or control.

Subnet
Subnet (short for subnetwork) refers to a distinct subdivision of an IP network, usually created for performance or security purposes. Subnets typically include the computers, systems, and devices in one location, office, or building, with all nodes sharing the same IP address prefix.

TCP
TCP (Transmission Control Protocol) is a network communications protocol which enables two host systems to establish a connection and exchange data packets, and ensures data is delivered, intact, to the correct destination. TCP is typically grouped with IP (Internet Protocol) and known collectively as TCP/IP.

UDP
UDP (User Datagram Protocol) is an alternative protocol to TCP that is used when reliable delivery of data packets in not required. UDP is typically used for applications where timeliness is of higher priority than accuracy, such as streaming media, teleconferencing and voice over IP (VoIP).

WAN
WAN (Wide Area Network) is a network that spans a relatively broad geographical area, such as a state, region, or nation. WANs typically connect multiple smaller networks, such as LANs (Local Area Network) and MANs (Metropolitan Area Network). The Internet is an example of a WAN.