SIENNA

NDI Network Device Interface CLOUD

Technology Overview

Gallery SIENNA London, England **T** +44 208 340 5677 sales@sienna.tv www.sienna.tv http://ndi.newtek.com

An IP Video Protocol which works today

NDI Protocol

The NDI (Network Device Interface) protocol has delivered broadcasters and video professionals with a practical, and useful mechanism to connect video software and hardware on a local area network. NDI carries high quality compressed video, uncompressed audio and bi-directional metadata over a TCP socket connection. NDI includes a very fast but good quality codec to allow low latency, low CPU overhead encoding and decoding to pass resolution, aspect ratio and frame rate independent video across existing gigabit networks. NDI Services are advertised with mDNS and are thus automatically discoverable by other NDI devices on the same LAN. A wide variety of products, and utilities exist to support the NDI protocol, including free utilities to create, and view NDI sources. NDI is offered to the world, without qualification and with a royalty free license by its creators, Newtek Inc.

- **Works perfectly on existing Gigabit LANs and high quality WIFI networks**
- **Compressed video - ProRes / DNxHD type quality**
- **Very fast, license free codec included - 250 fps HD encoding per CPU core**
- **~ 100mBit/s for HD, scalable to 4K and beyond.**
- **Low latency, typically about 1 frame**
- **Uncompressed multi channel audio**
- **Use bonjour discovery for very easy deployment**
- **Bi-directional metadata support**
- **Compatible with Mobile Devices - mobile phone NDI Camera products**
- **Embedded support for Alpha Channel on same stream using BGRA**

Unsurprisingly NDI has been rapidly adopted by hundreds of product developers and the end user installed-base of NDI now dwarfs that of all other professional IP video protocols combined.

NDI was designed for local area networks, using TCP sockets and bonjour (mDNS) service announcements. With the rapid adoption of NDI, customers are now beginning to ask for a mechanism to extend their NDI local area networks, over wide area and global networks. NDI.Cloud was created to meet this demand.

LAN to WAN Expansion of NDI

The Challenges

Whilst it might seem trivial to simply run the NDI protocol across a wide area network, there are number of important considerations which require an alternative mechanism.

- **NDI was Designed for Local Area Networks**
- **Uses TCP Protocol :**
  = suffers from B.D.P (Bandwidth Delay Product) over long distance latencies
- **100mBit/sec data rate (for HD) too high for many desirable WAN connections**
- **Bonjour service discovery doesn't propagate across typical WANs**
- **Requirement for grouping / routing of sources**

In order to provide a practical solution for NDI across wide area networks, NDI.Cloud carries the NDI video over an intermediate protocol which reduces bandwidth requirements, uses a reliable enhanced UDP transport to avoid bandwidth delay product restrictions, and exists within a software defined video network to provide virtual communities between sites, propagating source discovery across WANs.

The Solutions

NDI.Cloud uses the H.264 long-gop format as a mezzanine codec to carry the iFrame NDI video content across bandwidth restricted networks. This can reduce the required bandwidth to a range between 4 and 20 mBit/second which is controlled by the user based on available bandwidth and content type.

NDI.Cloud uses a reliable transport built on top of UDP which provides guarantee of data delivery, but does not suffer from the effects of latency and packet loss which can massively reduce TCP effective throughput when run over typical wide area networks.

NDI.Cloud gathers NDI service advertisements on each local area network and forwards them across the wide area network, to propagate the service discovery mechanism.

NDI.Cloud has a centralised web-based collaboration interface allowing users to create their NDI.Cloud wide area network - defining bandwidth for each site and relationships between sites using grouping.

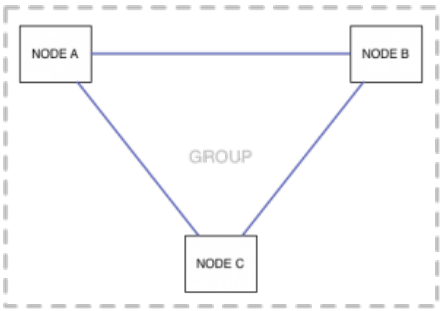
NDI.Cloud Infrastructure

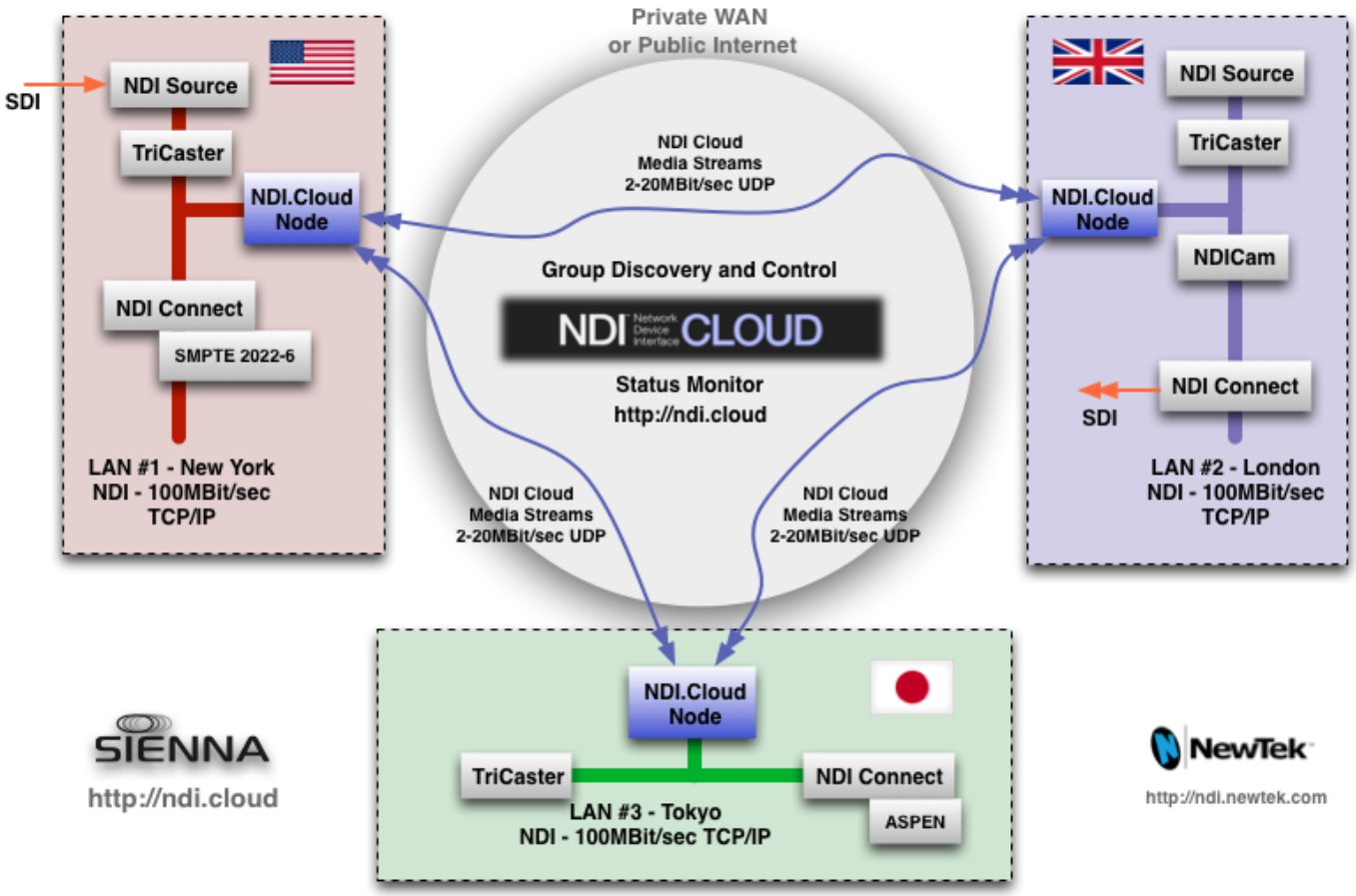
Functional Blocks

NDI.Cloud defines each Local Area Network as a **NODE**

Multiple NODEs are linked to form a **GROUP**

Groups can be **Private** or **Shared** with 3rd Party Nodes





Node Gateways discover one another via the central cloud database then begin direct peer-peer communication.

NDI Sources on each LAN are presented to WAN peers by the Node Gateways (in blue).

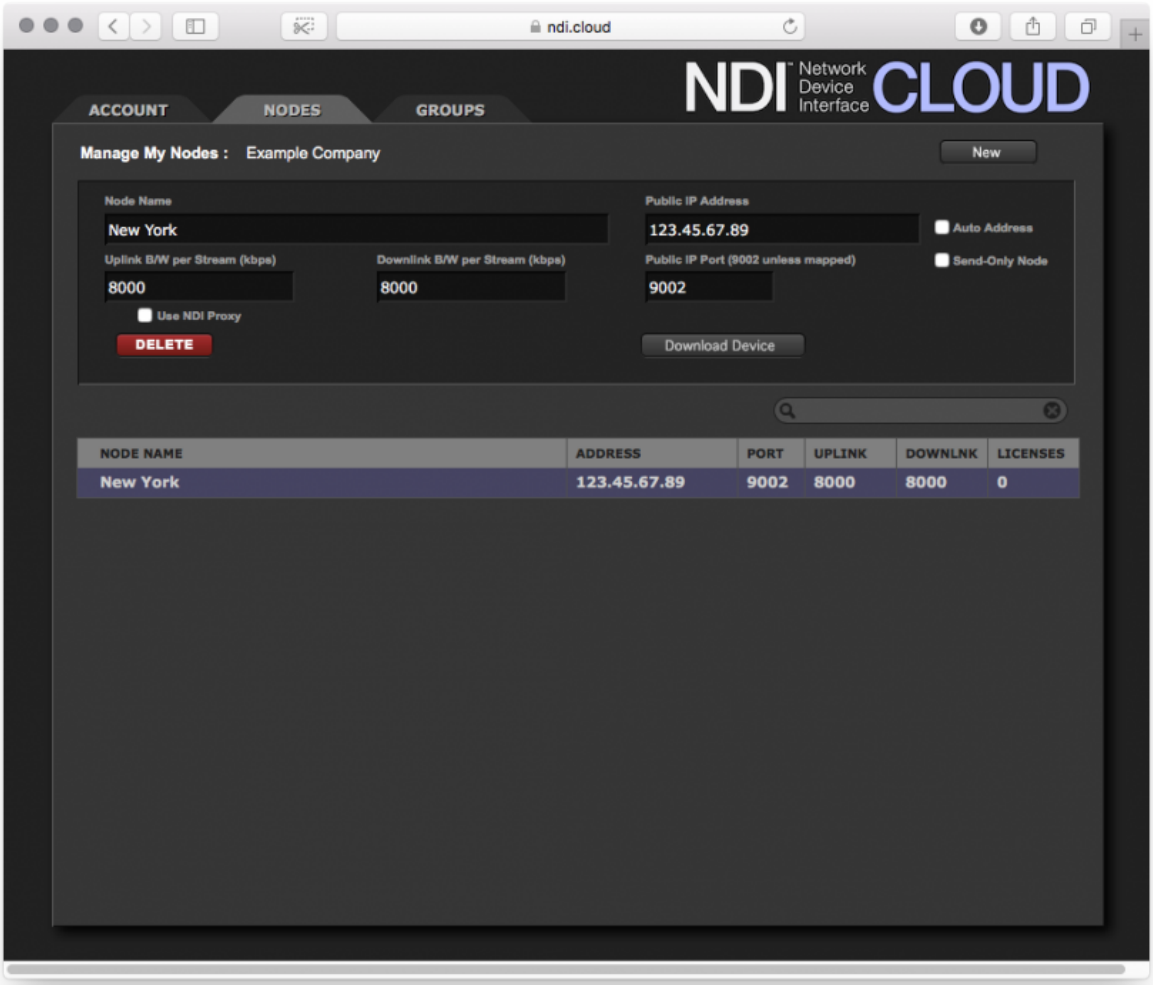
All video flows peer-peer - the Cloud database is simply for configuration and discovery.

Gateways can communicate across the open internet, via private links or via a VPN.

The User Experience

Central configuration in the cloud

The first step in constructing an NDI.Cloud wide area network begins with the website http://ndi.cloud. Here a user logs in and creates the NODES and GROUPS which define the network. This user-friendly web interface forms the core of the user experience for configuration.



Changes made in the central cloud database are propagated to remote Nodes within 2 minutes, allowing on the fly reconfiguration of your wide area network.

Collaboration with 3rd Parties

Shared Groups to connect different WANs

As discussed earlier, an NDI.Cloud network consists of your NODES, which are associated into GROUPS. By default this is an entirely private network, where your nodes can only talk to other nodes within the same NDI.Cloud account.

In some cases, it may be desirable to link one or more of your Nodes to an NDI.Cloud WAN belonging to a 3rd party - to facilitate an ad-hoc link-up such as a remote interview, or other interoperation.

NDI.Cloud provides a mechanism to create a ‘shared group’ rather than a ‘private group’ - to allow 3rd parties to connect their Nodes, given a unique group ID and secure password. Within minutes of creating a shared group, you can start to receive video from NDI sources on a totally different NDI.Cloud WAN. Just as easily you can terminate the ad-hoc relationship (as can the 3rd party).

Cross Platform Support

NDI Devices already exist on at least 7 different hardware / software platforms, including:

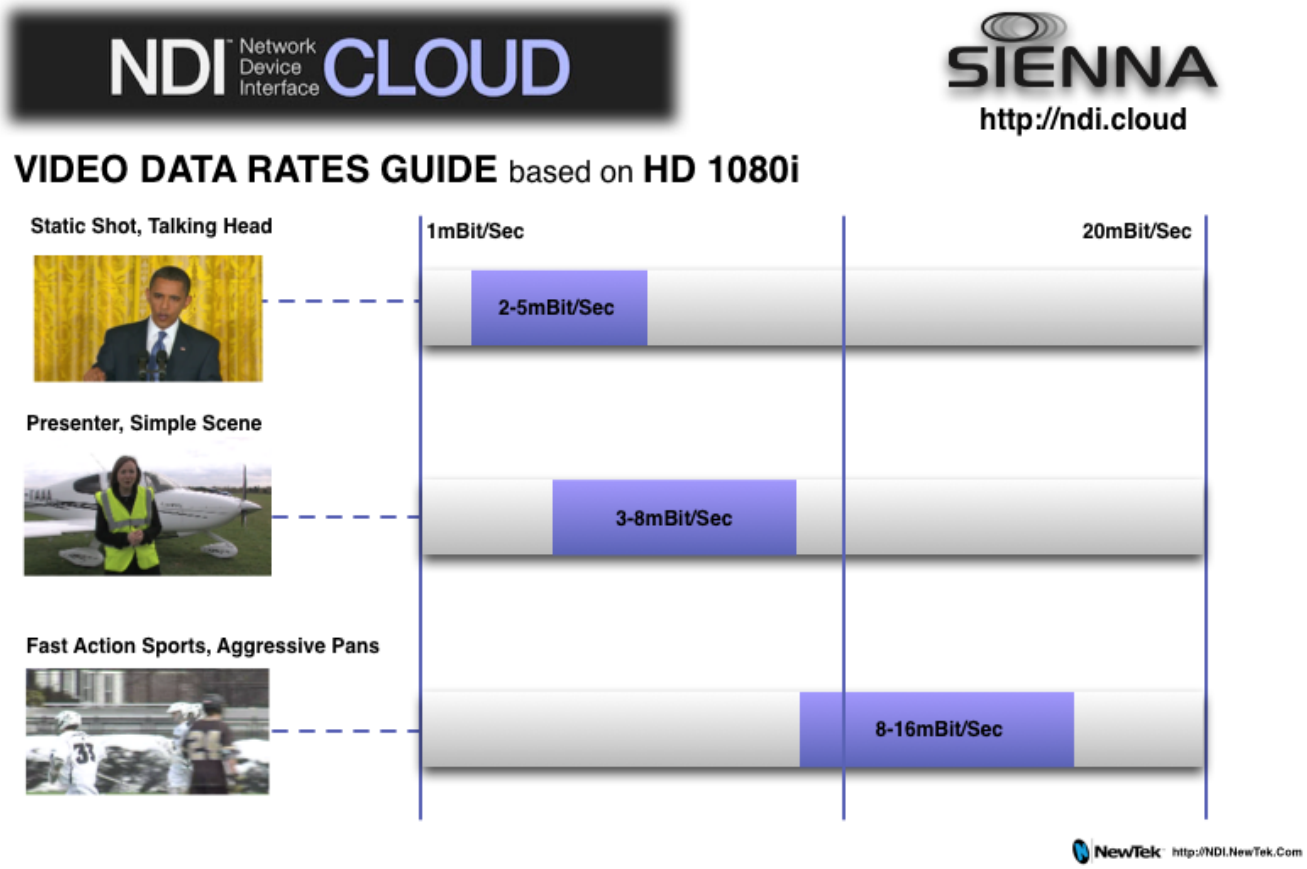
- macOS (OSX)
- Windows
- Ubuntu Linux
- iOS (iPhone, iPad)
- Android
- Raspberry PI
- Native FPGA hardware

The NDI.Cloud Node Gateway software supports all of the source and destination NDI platforms and can itself operate on 3 different platforms:

- macOS (OSX)
- Windows 64-bit
- Ubuntu Linux

Typical Data Rates for NDI.Cloud

Depending on the nature of the video content, and the image size, NDI.Cloud allows users to define an appropriate maximum data rate for the intermediate H.264 stream.



Latency

NDI.Cloud has been designed to limit latency wherever possible. The H.264 encoder is very low latency but of course a transit over the internet introduces both fixed latency based on distance, but also the need to compensate for fluctuations in packet trip-time, and also for packet loss which may require re-transmission of packets. Each NDI.Cloud Group defines a smoothing buffer which applies to all transactions between group members, and once again this is under the user control, and imposes a fixed smoothing latency period which allows for lumpy arrivals, and also for a resend period appropriate to the quality of the network connection (typically 2-3 times the ping time).

Where multi-cam sources arrive from the same NDI sending device, NDI.Cloud can resynchronise each channel to maintain frame accuracy between multi-cam sources.

Support for Alpha Channels

The base NDI protocol provides an option to send RGB+Alpha video frames in a single stream, allowing for transmission of key with fill.

NDI.Cloud maintains this capability across the wide area network by encoding the Key and Fill together within the same network packets. In doing so there is no risk of a timing offset between the Fill and Key data. Key data is encoded Luma-only since chroma is not relevant, and is thus very efficient and maintains good integrity.

Bandwidth Efficiency and Resource Control

When an NDI source advertisement is propagated across the NDI.Cloud WAN, it becomes a virtualised local NDI source on the partner network. However at this point, no data is flowing, and no bandwidth is consumed. It is not until a demand is created on the partner network by a receiving NDI device connecting to and consuming the virtual NDI source - that the actual transmission of data begins (which includes the encoding and decoding load on the Node Gateways). This mechanism allows for many NDI sources to be made available to WAN peers, whilst the network connectivity may only support a smaller number actually flowing. The NDI Source whitelist described on the next page can be used to limit the number of sources made available and thus the potential network load.

Security

The central NDI.Cloud database uses a TLS https interface to allow secure communications with web clients configuring a network, and with the Node Gateway servers who query the database to discover their peer Nodes. The central database uses salted encryption to secure login passwords, and it employs sql injection defences.

Nodes maintain a strict list of their partner Nodes, and each attempt to connect from the outside is compared with the known partner list before a connection is accepted.

Communications between peer Nodes can also be fully encrypted if necessary by deploying a VPN such as Hamachi to connect Nodes to one another. The NDI.Cloud intermediate protocol is defined with ethernet packets of 1404 bytes, to allow for the insertion of a 96 byte VPN wrapper without breaking existing packets into 2.

If Nodes do not want to offer up ALL their NDI Sources to peer Nodes, a whitelist function allows each Node to limit propagation of NDI sources to a fixed list of named sources.

For More Information:

For NDI.Cloud, contact:

Gallery SIENNA, UK

sales@sienna.tv

+44 208 340 5677

http://ndi.cloud

For the NDI Protocol contact:

NewTek Inc

http://ndi.newtek.com