What's New in NMOS?
A Tutorial on the Latest in Video over IP Control and Security

Jed Deame, CEO
Nextera Video

Outline

• What’s New with What’s Old
  – IS-04 (Registration & Discovery)
  – IS-05 (Connection Management)
  – Gap Analysis

• What’s New
  – IS-08 (Audio Mapping)
  – IS-09 (System Discovery)
  – BCP-002 (Grouping)
  – BCP-003 (Security)
  – IS-10 (Authorization API)
What is NMOS again?

- NMOS is the Networked Media Open Specification, developed by the Advanced Media Workflow Association (AMWA)
- Delivered in the form of an open specification on the AMWA website
- Enables ST-2110 equipment to seamlessly interoperate across vendors and facilities
  - Brings push-button simplicity to Video over IP Routing

What does NMOS Do?

**ST2110 Controller**

- Node HTTP API
  - /souces /flows /senders /receivers /self /devices
  - Resource updates & incoming request handling
  - Control Logic
  - Parameter changes & status updates

- Content Transport
  - for example: RTP

- PTP slave
  - (time distribution to all components as required)

- ST2110 Hardware
How does NMOS Work?

• Through a set of Application Program Interface (APIs)
• Exposed via http as: \textit{http://<IP Address>/x-nmos/<API Name>/...}
• Examples:
  – \textit{http://192.168.10.2/x-nmos/node/v1.2/self}
  – \textit{http://192.168.10.2/x-nmos/query/v1.2/nodes}
  – \textit{http://192.168.10.2/x-nmos/channelmapping/v1.0/map}
  – \textit{http://192.168.10.2/x-nmos/channelmapping/v1.0/outputs}
  – \textit{http://192.168.10.2/x-nmos/auth/v1.0/certs}

The Basics of NMOS

IS-04/05 System Diagram

1. Sources automatically register with RDS
2. Control Panel gets list of devices from RDS
3. Upon button press, control system commands receiver to join the new multicast stream and leave the previous one
What’s New with What’s Old: IS-04 (Registration & Discovery)

Current version 1.3 (elevated Sept 5)

Consists of 3 API’s (Application Programming Interfaces)

- Node API
- Registration API
- Query API

### Latest IS-04 Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>v1.0</th>
<th>v1.1</th>
<th>v1.2</th>
<th>v1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core functions including basic queries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer to peer mode (Optional from v1.3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic connection management (Deprecated)</td>
<td></td>
<td></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>BCP-003-01 HTTPS and secure WebSockets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiplexed Flows (ST.2022-6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paged queries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced (RQL &amp; ancestry) queries (Optional)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for IS-05 connection management</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Support for IS-07 and future transports</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>BCP-003-02 Authorization signalling</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
What’s New with What’s Old: IS-05
(Connection Management)

• Current version 1.1 (elevated Sept 5)
• IS-05 is an API which provides the means to create a connection between Senders and Receivers
• Enables switching through “activations”
• Activations can be immediate, relative, or absolute
• Supports FEC and redundant streams

<table>
<thead>
<tr>
<th>Feature</th>
<th>v1.0</th>
<th>v1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core functions</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>RTP unicast and multicast support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bulk connection mode</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Scheduled activation mode</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>MQTT and WebSocket transports</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Support for supplementary externally defined parameters</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Gap Analysis

What’s missing?

1. Audio break-away routing
2. Mechanism to set global parameters for a system
3. Security

What’s New: IS-08 (Audio Mapping)

Audio routing/shuffling facility with 4 APIs:
- Inputs
- Outputs
- Map
- I/O

Provides SDI-router-like capabilities
- Combine individual channels from multiple sources into any output
NAB IP Showcase
IS-08 Audio Demo

• Multi-vendor demonstration of Audio Mapping
• 3x 16-channel Senders
• 2x 16-channel Receivers

IS-08 Mapping Controls
What’s New: IS-09 (System Resource)

- Provides a single API resource (via the path /global) with the following:
- “System ID”, assigned randomly at each facility
- Protocol: http or https
- Version: Indicate NMOS API versions supported
- Server Priority: Helps with Bonjour/Avahi discovery
- Extensible for DNS-SD Advertisement of system resources such as RDS (Registration and Discovery Server)
What’s New: BCP-002 (Grouping)

- Best practices for grouping NMOS resources
- Uses the 'tags' resource in IS-04 in order to achieve 'natural grouping' of Senders and Receivers
- Ex) Video, Audio, and ANC from a specific device
- Uses “grouphint” tag

Grouping Example
Playout server sender with 1 video & 2 audio flows

Video 1 group: “Playout Master”
Video 1 role: “Primary”

Audio 1 group: “Playout Master”
Audio 1 role: “Audio 1 – 2ch”

Audio 2 group: “Playout Master”
Audio 2 role: “Audio 2 – 5.1ch”
What’s New: BCP-003 (Security)

BCP-003-01
Uses Transport Layer Security (TLS) in order to encrypt communications between API servers and their clients (https)

BCP-003-02
(Work In Progress) covers client authorization for the NMOS APIs.
What’s New: IS-10 (Authorization API)

- Accompanies the BCP-003-02 specification to restrict what users are authorized to change in an NMOS system.
- Work in Progress

Exposes /register_client endpoint

Discoverable using unicast and/or multicast DNS using the '_nmos-auth._tcp' service name

Requires the use of TLS when sending requests using password authentication (https)
Public Key Infrastructure (PKI)

- A set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption

NMOS BCP-003-02 Example

- Authentication Server
- Broadcast Controller
- IP Source
- IP Destination
- Public Key
- Token (JWT)
- Activation (JWT)
- Essence Flow (2110)
Core Technologies

PKI (Public Key Infrastructure)

HTTPS (http over TLS)
Connection Security (Encrypted Control Signals)

REST (HTTPS PUT & GET)

JSON (Key-Value Parameter sets)

OAuth 2.0 (Open Authorization)
Clients Authenticate with Authentication Server

JWT (JSON Web Token)
Client Authorization (issue access tokens) – RSA with SHA-256

NMOS Security Goals

Confidentiality - Data passing between client and the APIs is unreadable to third parties.

Identification - The client can check whether the API it is interacting with is owned by a trusted party.

Integrity - It must be clear if data travelling to or from the API been tampered with.

Authentication - The client can check if packets actually came from the API it is interacting with, and vice versa.
**NMOS Cipher Suite**

- TLS ECDHE ECDSA WITH AES 128 GCM SHA256
- TLS ECDHE ECDSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 128 CBC SHA256
- TLS ECDHE RSA WITH AES 256 CBC SHA384
- TLS DHE RSA WITH AES 128 GCM SHA256
- TLS DHE RSA WITH AES 128 GCM SHA384
- TLS ECDHE RSA WITH AES 128 CBC SHA256
- TLS ECDHE RSA WITH AES 256 CBC SHA256
- TLS ECDHE ECDSA WITH AES 128 CCM 8

---

**Johnny Quest Decoder Ring:**

TLS = Transport Layer Security  
ECDHE = Elliptic Curve Diffie-Hellman Ephemeral KE  
ECDSA = Elliptic Curve Digital Signature Algorithm  
AES = Advanced Encryption Standard (#bits)  
GCM = Galois/Counter Mode  
CBC = Cipher Block Chaining (XOR)  
SHA = Secure Hash Algorithm (#bits)  
CCM = Counter with CBC-MAC (Cyber Block Chaining Message Authentication Code)

---

**Customer Case Study – Secure KVM**

![Diagram of Secure KVM setup]

- SDI Sources
- 1 Gb/s Switch Fabric
- SYSTEM MANAGER
- Remote Monitor
- RX GW
- TX GW
- SERVERS/Workstations
- Optionally Encrypted Video/Audio/USB

**Secure Control**

**User Authentication**

---

Curated by Video Services Forum vsf.tv
Summary

- NMOS IS-04 & IS-05 are solid, stable, and mature
- They are employed in most all new SMTE 2110 products
- New features like IS-08 (Audio Mapping), IS-09 (System Discovery), and BCP-002 (Grouping) take NMOS to a new level, surpassing the level of control provided in SDI
- BCP-003 (Security) adds a layer of security that has been sorely needed in control systems for quite some time
- NMOS is the glue that holds an ST-2110 environment together and enables extraction of new business value

Thank you

Jed Deame, Nextera Video
sales@nexteravideo.com, 650-600-9686

Thank you to our Media Partners