THE BROADCAST BRIDGE

Audio Over IP Primer For Broadcast

Essential Guide

EG
ESSENTIAL GUIDES

Introduction

IP is relatively new to broadcast television as the network speeds needed to make video over ethernet distribution operate reliably, are only just emerging. But sending video is only half of the television story and many would argue, from the perspective of the human visual and auditory system, that audio must be more reliable than video.

The good news is that audio in the IP domain has been available for nearly twenty years and vendors have solved many of the challenges that are now presenting themselves to broadcasters. Seamless integration and interoperability are a given, and plug-and-play is a reality.

But to deliver this level of interoperability and reliability, a great deal of work goes on under the hood. With a whole plethora of differing combinations of bit depths, data rates, and channel configurations, entire protocols have been built to allow senders and receivers to navigate these challenges and exchange reliable audio.

Security is growing in prominence and broadcast engineers are asking very searching questions. So now we must think beyond network security and firewalls so systems can reliably operate and be used.

Vendors providing audio over IP solutions have been consistently making IP work for many years and integration is second nature to them. In this Essential Guide, we will investigate the lessons we can learn from audio over IP.

Tony Orme
Editor, The Broadcast Bridge

Tony Orme.

Audio Over IP Primer For Broadcast

By Tony Orme, Editor at The Broadcast Bridge

Part 1

Our auditory system is incredibly sensitive to the smallest sound distortion or discontinuity. Even the slightest audio pop, stutter, or level clip grabs our attention and distracts us from the television or radio program. Consequently, vendors working in the audio space, especially in IP, have spent years refining their Audio over IP solutions to make the sound clear and distortion free, as well as easy to use.

The ratio of audio channels to video in a broadcast service can be very high. Multilingual localization, audio description, and immersive audio are all contributing to increased demand for more audio channels. Intercom further inflates this requirement, especially when we introduce clean-feeds for outside broadcasts.

Over the years, a plethora of standards have emerged to increase the number of audio channels that can be distributed over single cables. This is especially important for outside broadcast vehicles where weight restrictions place limitations on the amount of heavy copper cable that can be installed.

Increased Complexity

As the number of channels available in a cable increased, so did the complexity of the infrastructure. MADI is a prime example of this. Although 64 channels can be accommodated in a single cable, the system is time-division multiplexed and broadcast specific audio-channel embedding and de-embedding equipment is needed, and complex switching matrices are required to route the signal.

SDI is also capable of inserting audio into its transport stream but a similar embedding and de-embedding challenge manifests itself. Furthermore, system designers are restricted to sending the audio to the same destination as the video. Again, complexity and costs soon escalate due to the bespoke requirements of switching, embedding and de-embedding.

All this results in restricted operation and increasing costs.

Asynchronous Operation

IP helps to overcome these challenges as it is much more flexible and scalable than SDI, AES, or MADI. Although IP also uses time-division multiplexing, it assumes asynchronous operation so packets can be inserted and extracted from the transport stream without the tight tolerances imposed by a synchronous distribution system.

One of the major benefits of IP is that it is essentially a software protocol definition and assumes nothing about the underlying hardware distribution system. Many broadcasters use Ethernet to transport IP, but it is not mandatory. This is also one of IP's greatest benefits as it is transport stream agnostic and can be distributed over many different types of physical network.

Furthermore, the IT industry has been using IP and Ethernet for over thirty years, even though the data-rates were only a few megabits for early adopters. Consequently, researchers and IT professionals have had the best part of fifty years to understand, improve, and design faster and more reliable networks.

AUDIO STREAM

Bit depth	**-**	**16bits**
Sample rate	**-**	**48kHz**
Bit rate	**-**	**16 x 48k = 768,000 bits/sec**

ETHERNET LINK

1Gbps	**-**	**80% data utilization = 0.8 x 1,000,000,000 bits/sec = 800,000,000 bits/sec**

NUMBER OF AUDIO STREAMS

Ethernet data utilization / audio stream bit rate = 800,000,000 / 768,000 = 1,042

Therefore, 1,042 audio streams can be transported on a single 1Gbps Ethernet link

Table 1 – Calculations showing audio capacity of a 1Gbps Ethernet link, as Ethernet is by-directional, 1,042 audio streams can flow in each direction, this is equivalent to 16 send and 16 receive coaxial cables (32 in total) for MADI.

Thousands of scientific papers currently exist demonstrating the massive amount of research that has gone into IP and Ethernet network optimization and improvement.

This has further led to vendors outside the broadcast industry designing and building improved networks and connectivity. In 1983, Ethernet speeds of 10Mbps were the norm, but now, the IEEE expect to release the 400Gbps by 2021 (IEEE 803.2cu).

AoIP started to make massive inroads into broadcasting about twenty years ago as network data throughput and reliability improved. Although uncompressed audio has a much lower bandwidth and data-rate requirement than video, even a single sample loss can be detected by the human ear, this meant networks had a very high-performance bar to achieve.

Bi-directional Data

The vast majority of transport standards used with IP are bi-directional. That is, the equipment at either end can both send and receive simultaneously. This is a big change for broadcasters as video and audio systems operate in one direction with point-to-point connectivity.

Networked bi-directional signal flows open up a fantastic array of opportunity for broadcasters as they can now maintain both full duplex signal exchange and control between devices. For example, a microphone can be muted from a remote location using a control system based on a TCP/IP protocol.

A single 1Gbps ethernet link can transfer in excess of 1,000 audio channels (assuming 80% network utilization for frame and packet header overhead and preambles, and 16bit audio sampled at 48KHz).

One of the challenges AoIP pioneers had to overcome in the early days of its adoption was signal interoperability. The big advantage of synchronous networks such as MADI, AES, and SDI, is that the audio signal specification is well defined, that is, the sender and receiver know exactly what types of signals are being exchanged.

Improve Flexibility

Synchronous, rigid transport streams have served the broadcast industry well for many years, but they lack flexibility and scalability. If we are to get the best out of IP, then we cannot conform to these intractable standards and must think beyond them.

If a microphone is configured to send 24bit audio at 96KHz sampling, we cannot assume the receiver knows this. If it is configured to accept 16bit audio at 48Khz sampling then the receive engine probably will not sync up to the audio, and even if it does (by chance), the resultant signal will be a cacophony of acoustic distortion and chaos.

Furthermore, how do we know how many audio channels are associated with a specific stream? In the IP world, streams are identified by their IP source and destination addresses, protocol specifier, and stream type (multicast or unicast for example).

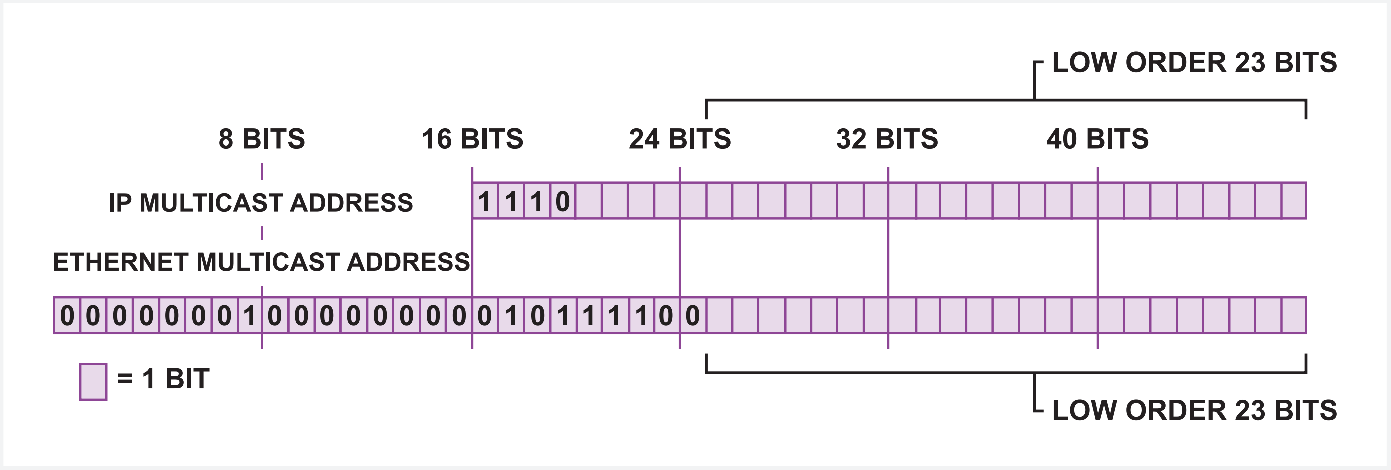


Diagram 1 – IP multicast addresses in the range 224.0.0.0 to 239.0.0.0 are mapped into the reserved Ethernet MAC address range 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF.

It is possible for a broadcaster to manually configure a system. The IP addresses will be known during system installation and the associated bit depths and sample rates. However, manual configuration is an almost impossible task to maintain for any period of time. Soon after the infrastructure is built, operational requirements will demand configurations and signal routings are changed. With potentially hundreds of audio streams available on each Ethernet link, this is a daunting task with the significant potential for human error.

One-to-Many Distribution

Audio over IP distribution has the option of using unicast or multicast. The lower data rates in audio make multiple distribution of audio streams achievable as they tend to be in the order of one or two megabits per second as opposed to several gigabits per second in uncompressed video.

Audio unicast is easier to implement than multicast and is often used in AoIP where adequate bandwidth headroom is available and predictable.

Multicast is the IP version of the distributing amplifier and is a bit-rate bandwidth efficient method of providing a one-to-many mapping of a single source to multiple destinations. Down-stream devices opt in and out of the multicast stream and the ethernet switch duplicates frames and sends them to the appropriate port.

Multicasting soon becomes complex and difficult to manage with a typical facility providing thousands of streams.

The good news is, the pioneers of broadcast AoIP have found a solution to managing these systems and we discuss this further in Part 2 of this Essential Guide.

Synchronous distribution transport streams have the signal timing built into them. For example, AES3 embeds the sample clock into the transport layer using the “bi-phase mark” encoding method. This guarantees that the receiving device can lock to the senders’ sample and bit clock to guarantee full signal reconstruction. However, the price we pay for this is lack of flexibility and scalability as the facility is limited to a very narrow subset of audio standards.

Clock Removed

Asynchronous distribution using Ethernet, or similar, strips away the underlying clocking system found in transport layers such as AES3, SDI, and MADI. But we still must synchronize the receivers sample clock to the senders otherwise samples will be lost or duplicated. Early audio streaming solutions used RTP (Real Time Protocol) to achieve receiver synchronization. PTP (Precision Time Protocol) was later adopted to maintain higher levels of synchronization leading to high standards of signal reconstruction.

PTP requires a master clock generator to allow send and receive devices to synchronize. As far as PTP is concerned, the connected devices such as a microphone and sound console, are slaves to the PTP master. In AoIP systems with up to one-hundred devices, local PTP clocks can be generated using one of the sound devices, so we don’t need a separate master generator.

Synchronize Clocks

Buffers are a fundamental requirement of any asynchronous system. The assumption is that the sender and receiver sample clocks are frequency and phase synchronous in the long term and PTP provides this for us. However, anomalies in the network can lead to packet reordering and temporal shifting leading to packet jitter. Buffers will solve packet jitter issues but they lead to excessive latency if they are too big or incorrectly used.

Again, PTP can be manually configured along with buffers but systems become incredibly complex very quickly and an automated version of connectivity better serves the facility, and we discuss solutions for this in Part 2.

Vendors working in the AoIP field have been developing solutions to address the challenges discussed here for twenty years. Consequently, they’ve had a great deal of opportunity to solve many of the challenges broadcasters face when moving to IP infrastructures. In Part 2 of this Essential Guide, we investigate the tools needed to automate interoperability for seamless connectivity.

Part 2

In Part 1 we introduced the benefits of Audio over IP and investigated some of the subtleties that make it the ideal choice for modern broadcast facilities. In Part 2, we look at the practicalities of making AoIP work in a real-time television environment.

Plug-and-play has been available in IT systems for many years. When we walk into a café the WiFi just works, or when we insert a USB drive to a computer it appears in the file viewer almost instantly, even automatically downloading and installing the drivers if needed. Adding a video card or external GPU requires little input from the user, again, it just works.

It hasn't always been this way. When home computing and IT was in its infancy, even making a simple home network seemed to be incredibly difficult. Drivers had to be manually downloaded and hours were spent configuring files to recognize USB and network devices. Adding a new video card seemed like an impossible job.

Thirty Years of Experience

As audio over IP has been around for nearly thirty years, there has been plenty of opportunity for vendors to fine tune their systems to make interoperability much easier to achieve.

Just like IT, audio over IP has network and open standards solutions.

Audio has a multitude of configurations. From the number of channels to the sampling rate, and from the bit depth to the endianness of the data format, and that's before we start even considering compression and coding types.

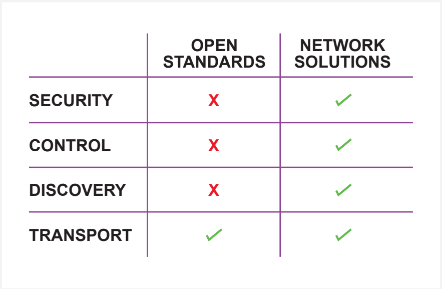
A microphone connected to an IP network stream will need to be configured so that any device receiving its IP packets can make sense of the audio. An IP stream of audio, by default, doesn't have any knowledge of the audio sampling rate, bit depth, or channel configuration. The act of streaming audio at an IP packet level only occurs at the transport level.

Plug-n-Play Solution

To provide a complete plug-and-play system, further features are required such as discovery, control, and security. As well as telling a downstream device how the audio is configured in the IP stream, there must be a method of determining its existence on the network as well establishing its IP address.

Broadcast systems tend to work within managed networks. This provides us with some assurances such as minimal latency and ringfenced security, but some administration is still needed to allocate IP addresses, systems such as DHCP.

AES67 is a form of an open standard. The documentation of the standard mandates a specific RTP payload format for delivering audio over IP as well as methods of exchanging parameters about the audio stream. However, it does not discuss anything about discovery, or control.



	OPEN STANDARDS	NETWORK SOLUTIONS
SECURITY	✗	✓
CONTROL	✗	✓
DISCOVERY	✗	✓
TRANSPORT	✓	✓

Diagram 1 – Providing an open transport standard is often only the beginning, the whole solution includes discovery, control, and security.

Discovery is a complex service within the network and helps make the whole configuration of the system dynamic and much easier to manage. DHCP (Dynamic Host Control Protocol) is used in IT systems to issue and retrieve IP addresses for devices connected to the network and then removed. The system administrator provides a range of IP addresses available to the DHCP that it uses.

In audio over IP, the challenge of providing IP addresses is further complicated by the addition of multicasting. Not only does a management system have to issue IP addresses, but it must also manage the allocation of multicast addresses. Although there are several million addresses available within the range, downstream devices must know the multicast IP address to connect to the service.

For example, if Presenter-A's microphone uses multicast address 224.0.10.0, then a sound console requiring Presenter-A's microphone stream must first know it exists, then know the format of the audio stream, and then indicate to the Ethernet switch that it requires a copy of the stream. This could all be administered manually with a spreadsheet keeping record of the parameters, but even the smallest system soon runs into many hundreds, if not thousands of active multicast streams in a network.

Although plug-n-play solutions deliver fantastic ease of use, interoperability with other formats such as MADI, AES3 and AES67 are required. Plug-n-play systems allow manual configuration of the management software to facilitate other formats that don't strictly adhere to their protocols.

Increased Flexibility

The upside of this type of configuration is that the facility becomes incredibly flexible but the price we pay is significant complexity. Even if we assume a multicast source is known either through an SDP file (Session Description Protocol) or is fixed, the task of entering every multicast stream IP address into a device is an incredibly difficult task fraught with potential for error. This is further complicated when using assignable sound consoles where the parameter configuration may be buried deep in a menu structure.

Even with this very simple example, we can see automated discovery and interoperability is a very difficult task to get right, and open standards bodies such as the AES seem to have stayed away from specifying it in the AES67 standard.

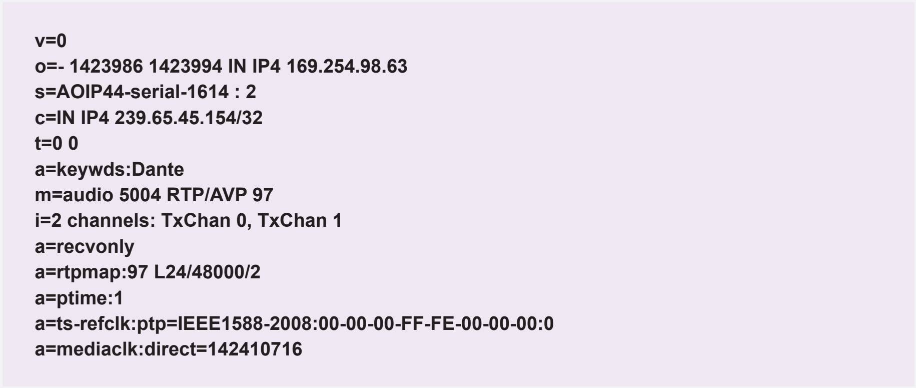
Interoperability Testing

One of the biggest challenges for achieving discovery and interoperability is the ability to test many different vendors software implementations so they work together. Many vendors put massive amounts of time, energy and resource into making their products work, and they simply don't have the time to release highly skilled R&D teams to go on interop-days to see how reliably their equipment connects with a competing-vendors. This is before we start even considering the potential for commercially sensitive source code to be exposed to multiple vendors.

This is one of the reasons vendors like to provide their own discovery and interoperability management systems. SDI, AES3 and MADI are all effectively transport layer distribution systems. Yes, we can connect an AES3 disk player to an AES3 sound console and we know it will work, but this is an extremely rigid way of working as the broadcaster is limited to a very small subset of audio standards. If we want to take full advantage of the flexibility and scalability IP offers then as users, we must make some compromises. For example, we should accept vendors will provide vendor specific solutions especially as we move into automated management of networks. In fact, if we want reliable systems, we should encourage this.

With AES67 at the transport level and vendor specific management and control for discovery and security, we have the best of all worlds. It would certainly be possible for multiple vendors to get together to build an open discovery, control and security protocols, but it would take an age to deliver such complexity.

Furthermore, today's agile development demands software versions are released quickly to deliver maximum functionality and features for the users, but this would be almost impossible for multiple vendors developing new management layers. It is possible, but very inefficient.



```
v=0
o=- 1423986 1423994 IN IP4 169.254.98.63
s=AOIP44-serial-1614 : 2
c=IN IP4 239.65.45.154/32
t=0 0
a=keywds:Dante
m=audio 5004 RTP/AVP 97
i=2 channels: TxChan 0, TxChan 1
a=recvonly
a=rtpmap:97 L24/48000/2
a=ptime:1
a=ts-refclk:ptp=IEEE1588-2008:00-00-00-FF-FE-00-00-00:0
a=mediaclk:direct=142410716
```

Diagram 2 – sample SDP (Session Description Protocol) file showing the audio and IP parameters.

Delivering Security

Using vendor specific network management for audio over IP gives vendors much more freedom to deliver reliable and secure systems with a host of regular new feature sets. Software can be developed and tested within the confines of a well understood system, and bugs can be detected quickly and dealt with efficiently.

Also, standards tend to be designed by committees. Although these groups usually consist of dedicated and talented CTO's, each will want to move the specification to their point of view. This is not to suggest any CTO is better than another, it's just that they have different ways of thinking and approach solving problems from different frames of reference. Consequently, open standards, if left unchecked, have the potential to balloon and fill with inefficient compromise to keep everybody around the table happy.

Committees are, however, very good at forming new well-defined standards. A typical example of this is the ST2110 and AES67 suite of specifications. There is just enough specified to make them efficient, but not so much that they become overweight and cumbersome.

Best of All Worlds

Solutions providers are constantly developing and supporting the critical discovery, routing and security tools needed by the broadcast industry. While "raw" interoperability standards such as AES67 can be configured manually and used in less complicated systems, this is not the intended use case and is unlikely to be sustainable or scalable as discussed earlier. Fortunately, most third-party developers of integrated and complete AoIP systems incorporate support for these standards, freeing broadcasters to choose the components they prefer while maintaining complete transport flexibility.

This operational method has been well established by vendors working with audio over IP for over twenty years. They seem to have reached a compromise where they provide all the advantages of discovery, management, control, and security, while simultaneously delivering interoperability and connectivity to licensed third party devices. These partner-vendors have direct access to the R&D teams to help them provide fast and efficient solutions, as well as identifying any anomalies along the way. All to the benefit of the broadcaster.

In Part 3 of this Essential Guide we look at system management and network security.

Part 3

In Part 2 of this Essential Guide we looked at solutions to keep AoIP systems simple and discussed the compromise and efficiency vendor specific network systems provide. In Part 3, we look further into system management and network security.

Traditional SDI, MADI, and AES broadcast infrastructures using point to point connections have the advantage that it's relatively easy to work out where signals are being routed. The downside is that cable looms suddenly become very bulky and to achieve redundancy and improved reliability, complex redundant systems must be designed, further adding to the size and cost of wire looms.

Adding devices usually involves installing more cables and increasing the capacity of signal routers. This often leads to static systems that are difficult to scale and are challenging to adapt. When building a broadcast facility, how can you estimate with any level of certainty your resource requirements in five to ten years? Especially with technology progressing at the pace it is today.

Built in Redundancy

Networked IP systems, by their very nature, have built in redundancy and the physical cabling systems are significantly smaller than their point-to-point counterparts. Expanding routers and switches requires less forward planning because IP is data agnostic, so the same physical ports for video, audio, and metadata can be used. We don't need to worry about provisioning for specific audio, video, or control circuits.

Networked systems, by definition, do not employ point-to-point connectivity, so we often have to represent signal flows and devices in abstract terms to get a better understanding of them. Although network cables exist in the AoIP world, we don't generally follow system diagrams with cable numbers to get a sense of the system design. Point-to-point systems, although relatively static and inflexible, give a natural demarcation between functionality and locality. For example, each studio would be physically separated from another in terms of equipment and cabling.

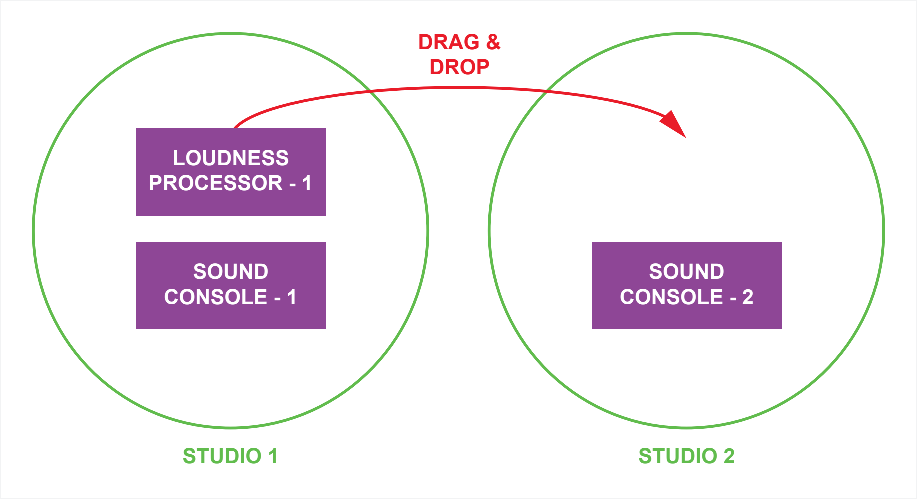


Diagram 1 – In IP, devices are abstracted from their physical presence so they can be moved to other domains. Here, two domains have been created, one each for studio 1 and 2. The Loudness Console, when not being used by studio 1 is dragged to studio 2. As well as providing this feature, the management software must make sure only authorized people have access to this facility.

Sharing Resource

In the IP world, multiple studios can easily find themselves sharing cables, switches, and infrastructure resource. Especially as we move more to virtualization. This is one of the great benefits of moving to IP as we can better utilize resource as it becomes sharable over many different locations.

To better understand networked systems, we can use logical grouping of resource. The concept of domains is well established in IP using address masks and VLAN segmentation. Using networked solutions, vendors provide methods of grouping devices into specific functionality. This helps engineers better visualize a system to assist with configuration and maintenance.

Organizing devices into domains is a logical solution and provides maximum flexibility. If a Loudness processor is currently grouped in studio-1's domain, then it can be easily moved to studio-2's domain to make it available as a resource should studio-1 not need it anymore. As well as providing greater flexibility, domain organizing further improves security for the broadcaster.

Security is a very emotive generic term and means so many different things. We may be referring to the prevention of outside hackers, or we may want to stop people inadvertently configuring systems in error, or we may not want one studio to have access to another studio's resource. Administering security is notoriously difficult as we first have to decide what we want when we talk about security.

Vendors have recognized the need for security in AoIP solutions and now provide several layers to keep systems secure. To understand this better we can look at how enterprise IT provides security.

Every device in an enterprise system, whether it's a desktop computer or switcher, requires the user to enter their credentials to access the resource. As well as stopping unauthorized access, it also provides a forensic audit trail showing who logged in and when. Access rights associated with a username further provides granularity so that specific users can only access authorized functionality within a resource.

Enforcing Authorized Access

The same is true for AoIP network solutions. Even devices such as microphones have parameters built into them that can be remotely controlled to improve their operation. To keep systems secure, remote login is used so that only authorized personnel can access the potentially sensitive control. This isn't just about stopping malicious hackers, this is also about stopping somebody who is trying to be helpful and starts trying to configure a device without the necessary skillset or experience.

One of the enterprise IT policies to keep facilities secure requires users to regularly change their passwords. LDAP (Lightweight Directory Access Protocol) is a centralized method of keeping a record of usernames and passwords. LDAP enforces the policies set by the IT manager and forces users to change passwords on a regular basis. However, trying to maintain multiple IT and broadcast infrastructure databases by keeping two sets of password policy rules is incredibly difficult, often resulting in the rules not being enforced on broadcast infrastructure resource.

To deal with this, vendors offering advanced AoIP network solutions provide a gateway to the enterprise IT central LDAP server. This means, the same username and password can be used by the engineer for both their IT and AoIP resource. As the AoIP management server queries the LDAP server when a login request is made for an audio resource, any change in password is automatically passed to it thus negating the need to keep two credential databases.

Access rights within the management software combined with the domain manager further refine the security of the system. Users within studio-1's domain for example, can be restricted to accessing and monitoring resource for just that studio. Although the network is available to all the studios in the facility, only those with access rights for that studio can access its facilities. Monitoring rights and configuration rights can be granted individually to improve security.

This may all seem obvious and in the enterprise IT domain these are well proven working practices. This level of access is also available in many broadcast devices and resource.

IT Integration

However, the key here is that vendors in the AoIP space have combined their solutions with the enterprise IT LDAP server to provide a fully integrated system. As usernames and password changes become automatically available in the AoIP manager, systems designers and integrators are more likely to use it.

This level of integration further includes monitoring and logging, both essential in maintaining systems and keeping them secure.

Enterprise IT managers often use infrastructure wide monitors such as Nagios and Paessler PRTG. These network monitoring tools probe servers, networks, and even applications running on servers to determine the efficiency with which they are operating. These dashboard monitoring systems quickly show errors and give easy access to deep menu structures, allowing engineers to dig further into individual servers, network devices, or other infrastructure equipment.

SNMP (Simple Network Management Protocol) is an internet standard for gathering data and monitoring managed devices on IP networks. They can even change parameters in these devices to fine tune their operation.

VM Improvement

Providing SNMP with its associated monitoring and control parameters on AoIP managers not only provides early alarms when an error occurs, but also provide a level of security as devices behaving erratically can be easily detected. This level of analysis is further improved if the management software is virtualized and running on a virtual machine (VM).

With the correct configuration, VM's can significantly improve security by providing a layer of access validation between the code and its underlying hardware resource. Hypervisor code running on the VM provides a level of abstraction from the underlying code so suspect scripts, device access, and memory violation requests can be quickly detected and blocked. This helps stop malicious scripts from running.

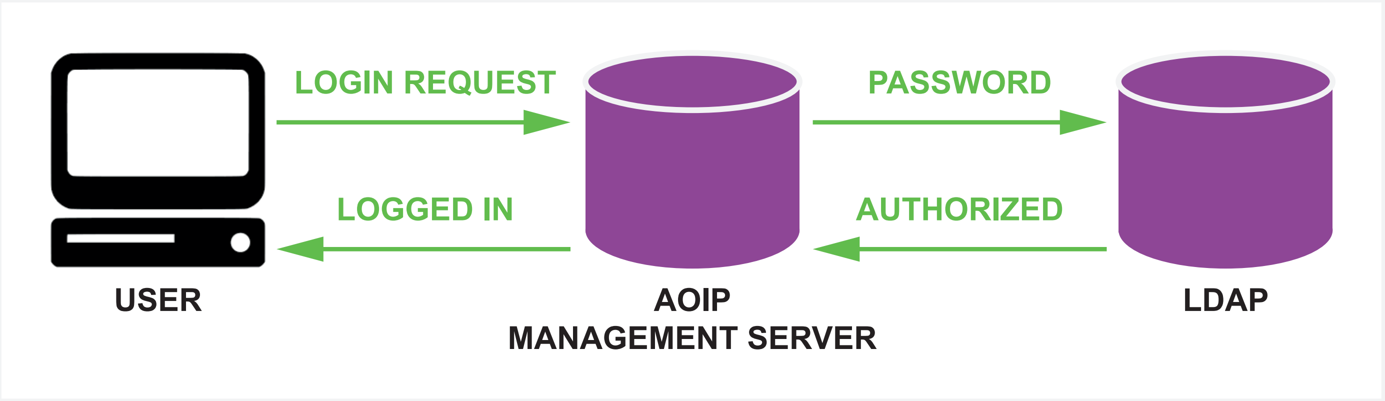


Diagram 2 – Light Directory Access Protocol (LDAP) is integrated into the AoIP management server so only one record of user credentials is kept to enforce authentication and security.

Throughout this Essential Guide we have seen how AoIP vendors, with their wealth of knowledge and experience, gained over the past twenty years have fine-tuned IP to work seamlessly for broadcasters. Not only have they been able to make systems work reliably, but they've gone the extra mile and integrated them into enterprise IT systems to provide efficient and easy to use solutions.

Reliable Integration is Key

Open standards certainly have their place and standards such as AES67 provide well defined solutions to specific transport challenges. It's only when we start moving up the implementation tree that we start to see the limitations of "design by committee" standards. Once we've got past the ability to move the signal data reliably across an IP network, we must turn our attention to integration.

Discovery, control, and security are incredibly important aspects of the total system integration and user experience. Reliability is more than just efficient signal flow; it also embraces the full operation of the system. We took this for granted with point-to-point connectivity, but if we want to take advantage of the flexibility and scalability of IP solutions, we must look to vendors who have brought all the different elements together and provided fully integrated solutions.

The Sponsors Perspective

An Introduction To Dante

By Brad Price, Senior Product Manager at Audinate

Dante audio networking is now well known in the broadcast industry. It is used by over 2100 products from more than 430 manufacturers, and is used in installations that range from broadcast studios and OB vehicles, to stadiums and recording studios, radio stations to schools and conference rooms.

Dante is far more than a transport protocol. It is a complete solution designed to provide every set of users with the tools they need to do their jobs easily and with confidence. From development kits used by manufacturers to the control and management tools for end-users, the solution is designed to ensure success and 100% interoperability between all Dante-enabled products regardless of brand.

Audinate firmly believes that IP technologies are the future of broadcasting, and that great user experience is what drives markets to embrace new possibilities. It's not enough to deliver high channel counts, ultra-low deterministic latency or sub-microsecond synchronization of all devices; it must make all this performance readily available to users without special knowledge or cryptic, fragile configurations. It must "just work" with exceptional performance right out of the box, like any truly mature technology should. In this paper, we'll examine the role of Dante's "full stack" approach in propelling networked audio over IP forward for broadcasters.

Supported by

Transport Layer and Interoperability

When transport works correctly, it becomes invisible to the user. As long as the system control interfaces remain basically the same, there is little reason for a user to be concerned. The transport layer is thus an area that can be changed without significantly altering the user experience, within limits.

Bringing that user experience to audio networking is largely what managed audio over IP is about. While Dante natively uses its own transport scheme that has been designed and proven for reliability and to implement features, other selected transport layers are also supported and are used to connect non-Dante devices to IP networks using familiar tools such as Dante Controller and Domain Manager.

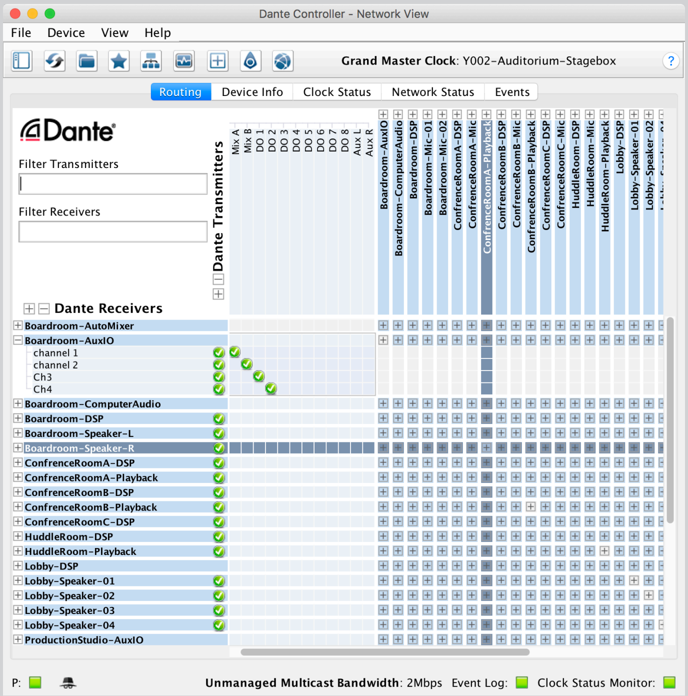
Dante supports the AES67 interoperability standard, which allows nearly any AES67-compliant device to connect to a network. Devices may send and receive AES67 and Dante audio and data simultaneously, so operators don't have to worry about vendor specific connections being affected by the introduction of another transport type.

As the configuration of SMPTE ST 2110 devices is quite complex, the Domain Manager provides tools to aid in this process. Once instated, devices can “speak” both native Dante transport and SMPTE ST 2110 at the same time, effectively converting synchronized audio traffic back and forth between the two. As with AES67, once SMPTE ST 2110 devices are setup, operators simply use the management controller to route signals easily and clearly.

Discovery and Control

In legacy non-networked systems, device discovery consisted of physically locating devices and connecting them with cables. The cable between devices defined not only the sole pathway between them, but also what type of signal was being carried. A cable carrying MADI wasn't doing anything else but MADI, etc. In networked systems, cables don't tell you what they are doing, and all devices are effectively all connected at once. Determining how devices are passing audio now becomes a crucial design element.

Automatic device discovery is an essential part of making a networked system truly workable. Without it, users would be forced to configure devices manually and determine settings by trial and error, adding friction and reducing chances of success. In contrast, when a user opens the management controller, they are immediately presented with a real-time view of the audio network as it is; all the devices, all the connections, all the settings and names.



Grand Master Clock: Y002-Auditorium-Stagebox

Unmanaged Multicast Bandwidth: 2Mbps

Dante Controller.

Once discovery is in place, there must be equally clear means of controlling the system for common tasks such as routing signals, changing sample rates or giving devices useful names. A single application provides all these elements with an easy-to-understand grid view that lets operators clearly see all devices and all transmit and receive channels. Simply clicking at the intersection of any transmit/receive pair creates a connection and audio beings flowing immediately.

While built on open standards, discovery and control tools are not specified in transport layer technology such as AES67 and SMPTE ST 2110. This is largely because those standards are intended to fill roles that solve particular transport interoperability problems, and no more. Easy, reliable discovery and control is key to driving the use of audio over IP.

Management and Observability

Transport, discovery and control are basic building blocks for any functional audio over IP system. Once that is in place, other questions arise: how does one monitor the status of the system? What happens if a device goes missing, or perhaps an unwanted device is added? How is clocking managed beyond any automatic settings? How can I organize my system around physical locations when the network shows me everything, all the time?

Dante Domain Manager is a server-based management tool to add layers of additional control, alerts, expandability and organization to allow:

- Organize your network into "domains" that represent groups of devices in physical locations, e.g., "Auditorium" or "Studio A".
- Work with domains one at a time for a clearer, easier view of a complex network.
- Route audio only within a domain for secure, non-interfering usage.
- Extend the network across subnets for nearly unlimited expansion over existing network topology.
- Instantly see the status of the network on the system dashboard, with instant notification of changes anywhere on the system, including device remove, device add attempted, subscription changes, clock failures and/or changes, etc.
- Receive alerts via email or SNMP when anything goes wrong or changes from previous state.

Security

The very good thing and the very bad thing about networks is that they make everything available at once. Good, because services can reach everyone, and bad because everyone can potentially reach things they shouldn't.

A network system demands network-style security. Fortunately, the IT industry has decades of experience in the deployment of computer systems from which to draw lessons and inspiration.

A security model that closely follows common IT practices is adopted, and starts with robust user authentication. Anonymous use is forbidden, and users see only the parts of the system to which they have permission as configured by the administrator.

User account administration is simplified by allowing Dante Domain Manager to synchronize with your existing LDAP or Active Directory implementation. Users may be granted any level of access on a domain-by-domain basis, from none to full control. All actions are logged and stamped with user name and time information, so troubleshooting is made easier and best practices may be more readily enforced.

Robust security needn't mean confounding users. All security is transparent to the operator and doesn't require expensive changes to tools or workflows.

Conclusion

The "full stack" approach taken by Dante provides users with a complete, fully supported toolset that lets them leverage the power of audio networking with low risks and the highest performance. With reliable discovery, easy-to-understand software and robust IT-style security, Dante takes the promise of networked transport and makes it a practical reality for nearly any user or organization.

Dante doesn't compete with open standards. Rather, it works harmoniously with open standards to provide value and functionality that standards alone only suggest can be done. It is built by a team who understands both the underlying technology and the problems faced by users in the real world, and who work to create products that are consistent and understandable. Dante exists to advance IP usage in the AV and broadcast worlds, simplifying product design for manufacturers and giving users a consistent way to use and manage networked audio across hundreds of brands.

12/2019

Supported by

Audinate®