WorldCast Systems
apt > acreso > audemat

The Essential Guide

To Audio Over IP

FOR BROADCASTERS



Powerful **Performance** | Powerful **Control** | Powerful **Savings**

CONTENTS

1. Why IP for Broadcast Audio?

2. IP Audio Applications

3. The Nature of Audio Over IP

4. About IP Networks

CONTENTS

5. Overcoming Imperfections

6. Advanced IP Concepts

7. Network Testing & Analysis

CONTENTS

www.worldcastsystems.com

A Little Bit **of Background**

It has been more than 12 years since APT designed and delivered the first audio codec that could transport high quality audio in real time over an Internet Protocol (IP) network. Back in 2003 ISDN was widely available and 950MHz and other analog microwave links together with E1/T1 were the accepted standards. Few broadcasters, if any, trusted or understood IP as a broadcast audio transport technology.

APT started its IP journey in a niche place with a very special customer, none other than SkyWalker Sound, the sound division of George Lucas Film based in Marin County, California. The SkyLink product was completely unique for its time; it was used as a tool by remote talent, producers or sound engineers to review a 5.1 mix over a managed IP link.

Together with the audio, an embedded SMPTE Timecode channel was transported to enable synchronization of the audio with the reels and rushes of film. While the SkyLink was well used and loved by SkyWalker, its appeal to others was limited as it required an expensive, managed IP network.

SKYWALKER SOUND
A LUCASFILM COMPANY

However, it became the cornerstone upon which APT began to build its reputation for IP Audio and the resulting expertise and in-house technology was used to develop globally successful, broadcast products such as the stereo Horizon and the multi-channel Oslo platform. Our current range of APT IP audio platforms (see page 68) continue to lead the field with the same commitment to audio quality, reliability and innovation that we had in those early years.

In this newly revised IP Booklet, revision four, we hope to provide a significantly expanded IP Audio primer.
The primer serves a number of functions: it gives a very gentle introduction to the concept of IP Audio and an introduction to IP networks and concepts and also offers practical advice on network testing and analysis both pre and post IP audio deployment.

The APT SkyLink
Both pre- and post-IP audio deployment

Also covered is some very specific information on networking for audio transport, covering optimum settings and configurations for typical broadcast uses and scenarios.

We trust that you enjoy this booklet and be sure to let us know what you would like to see in the next revision!

1. Why IP for Broadcast Audio?

Before the IP Revolution...

One thing that's clear from working in radio broadcast, broadcast engineers develop a deep fondness for the technology that has served them well down through the years.

Nowhere is this more true than in the niche part of radio broadcast that is audio distribution and STL (Studio Transmitter Links).

Name	**POTS / PSTN**
Also Known As:	Plain Old Telephone System / Public Switched Telephone Network
Description of Network	This refers to the use of narrowband phone lines for delivery of voice quality audio, limited to 8kHz Frequency Response and coded using ADPCM based G.711. Originally the POTS network was a collection of analog lines; today it will have a digital core with a mixture of technologies at the edges. These edge technologies are called the local loop or last mile and may still include copper wire but can also be microwave or fibre links.
Common Uses in Radio Broadcast	Remotes, Outside Broadcast, Audio Contribution
Advantages	Low delay, universally available, ITU-T Standardized
Disadvantages	Limited Frequency Response

Name	**ISDN**
Also Known As:	Integrated Services Digital Network
Description of Network  *APT's Original ISDN Codec, the DSM100 ProLink*	One of the first "high capacity" digital links to be made available to homes and businesses, back in the early 90's. The BRI (Basic Rate Interface) was by far the most popular access method for connecting ISDN codecs, comprising 2 B Channels at 64kBits with one D Channel. The typical ISDN codec from the early 90's was able to terminate a single ISDN line and therefore encode audio up to 128kBits.
Common Uses in Radio Broadcast	Remotes, Outside Broadcast, Audio Contributions, Studio Studio Links (SSL), (STL) Backup
Advantages	Low delay, reliable
Disadvantages	not universally available, expensive metered access

Name	950 MHz Licensed Microwave
Description of Network	In the USA, the Federal Communications Commission, FCC, licensed the 950 MHz band specifically for aural links for radio broadcasters. Within the 950 MHz band you have a 500 kHz channel.
Common Uses in Radio Broadcast	STL almost exclusively in the USA
Advantages	reliable, licensed
Disadvantages	small capacity, lack of available frequencies, Line of Sight required, subject to rain fade and other interference.

Name	X.21 / V.35
Also Known As:	Leased Line
Description of Network	Leased line circuits are delivered in increments of 64kBits and typical delivery speeds are 128kBits, 256kBits and 512kBits. The circuit is delivered with an NTU (Network Terminating Unit) and is a fully synchronous circuit. X.21 / V.35 is the protocol that is used to connect the Data Terminating Equipment (DTE) (in this context the codec) to the NTU on the circuit.
Common Uses in Radio Broadcast	STL, SSL, Audio Contributions
Advantages	reliable, low delay
Disadvantages	limited capacity, point to point circuit

Name	E1/T1
Description of Network	E1 is the basic 2.048 MBit building block of the synchronous network known as SDH that is used in Europe and the rest of the world for synchronous data delivery. T1 is the basic 1.548 MBit building block of the synchronous network known as SONET that is used in the US and Japan. Essentially the two systems are the same technically with a central clock keeping everything synchronized and a multiplexing hierarchy which assigns signals in to larger tributary groups and virtual containers. The key difference is the different size of the groups and containers.
Common Uses in Radio Broadcast	STL, SSL, Audio Contributions, National Networks
Advantages	reliable, low delay
Disadvantages	expensive, limited scalability, increasingly limited availability (in the US)

Reasons to Migrate to Audio over IP

You may have noticed that the term 'reliable' is used repeatedly when describing the technologies we have just outlined. While not immune to intermittent problems and outages, by and large all of these technologies have earned the reputation of being trusty stalwarts in the telecommunications world.

These technologies, which have served broadcasters for decades, are now being replaced gradually but in ever increasing numbers by IP. To migrate away from a tried and true approach, the reasons need to be compelling and below we examine some of the main advantages that are convincing Radio broadcasters to make the switch:

1 Flexibility

Flexibility is probably the key reason why an IP delivery method for audio is superior to any of the previous or existing technologies. You can generate and route additional channels easily using either multicast or multiple unicast technologies. A single channel encode can be decoded by tens of units (multiple unicast) or hundreds of units (multicast) and, if the network and hardware are available, this can all happen in an instantaneous configuration change.

The rigidity of synchronous networks and the point-to-point nature of microwave networks can never come close to this level of flexibility. The flexibility of IP connectivity has also made it easy to deploy live links on short notice, and international links where synchronous solutions might not be available for that location.

2 Cost

Critically, this flexibility doesn't add additional expense. Live and international remotes need no longer be the big budget events that they once were due to Telco costs. The combination of IP Audio together with a redundant streaming technique such as APT's SureStream (see page 69) enables

you to achieve T1/E1 quality and reliability for a fraction of the price.
For continuous and fixed operations such as STL and SSL, the cost savings of using IP as opposed to other technologies can also be significant over time. The example on page 10 is based on data provided to us by a US-based customer highlighting the savings they could achieve. While amounts may vary from country to country and region to region, the cost benefits in the vast majority of cases are significant enough to warrant a switch.

3 Scalability

Also related to the flexibility is the scalability of IP networks, particularly the ease with which you can scale your network up or down as well as the magnitude of the potential scalability.

Using multiple unicast or multicast you can easily and seamlessly add in an extra decode point or even ten extra decode points into your IP Audio network. As long as the IP network extends to that point, then connectivity is achievable.

4 Reliability (yes really!)

In the early days of IP Audio, reliability was the most common obstacle encountered when considering migrating to this type of network. Today most people accept that on a managed IP network with guaranteed bandwidth, QOS and an SLA, you don't have anything to worry about.

In the last couple of years, redundant streaming techniques such as APT's SureStream technology have achieved the same levels of reliability using only the public Internet.

5 Availability

IP is available almost everywhere via wired and wireless access points. You no longer need to book an ISDN or leased line drop to a remote broadcast site eight weeks in advance. However, the popularity of IP can cause some issues as increasing numbers of users crowd on to IP networks at sports venues, arenas and other sites. This particularly affects connections made over wireless networks, including 3G and 4G bandwidth. In order to compensate for this issue, advance capacity planning is necessary to calculate the connectivity required for an event and the numbers of users likely to be sharing the connection when you go live.

6 Control and Monitoring

If you can ping it, you can control it and monitor it. A fantastic by-product of the IP age is the fact that not only IP Codecs but Transmitters, Audio Processors, Consoles, Audio Routers, in fact, almost everything that makes up the air chain has or will have an IP interface. This allows the engineer not only the ability to control the operation from afar but to also jump into a situation and troubleshoot and make corrections remotely.

7 Network Consolidation

Consolidating everything to a single network type is beneficial in lowering costs and in increasing in-house knowledge and support of these business critical networks. However while consolidating all networks in your radio broadcast facility to IP can be advantageous, most users choose to have either a physical or virtual separation of these networks, divided between perhaps, office LAN, VOIP and Audio Over IP.

Potential Cost Savings from Switching from T1 to IP

Coast to Coast		Install	Monthly Cost	12 Month Cost	24 Month Cost	Average Annual Saving (after 2 years)
Link Only Comparison	T1 Line	$1,000	$1,600	$20,200	$39,400	**Save $17,800**
	MPLS	$750	$1000	$12,750	$24,750	**Save $10,500**
	2 x IP Links (Verizon FIOS, 3 MBits Down / 786 Kbits Up)	$0	$156	$1,872	$3,744	

Coast to Coast		Install	Monthly Cost	12 Month Cost	24 Month Cost	Average Annual Saving (after 2 years)
Link & New Equipment Investment	T1 Line	$1,000	$1,600	$20,200	$39,400	**$14,800**
	MPLS	$750	$1,000	$12,750	$24,750	**$7,500**
	2 x IP Links + 2 x WorldCast Horizon NextGen	$5,960	$156	$7,832	$9,704	

Potential Cost Savings from Switching from T1 to IP

8 Skills Consolidation

As already alluded to in a number of points, IP is here to stay. Like FM it could just be a 100 year technology, we are already 45 years on from the first packet-based switching proof of concepts and the ARPANET! The **A**dvanced **R**esearch **P**rojects **A**gency **N**etwork (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

We see today that almost every new piece of broadcast equipment has an IP interface and we are witnessing the demise of many other types of communications networks in favor of IP. So, whether you are a Chief Engineer or a student of radio broadcast, knowledge and proficiency in the field of IP networks and networking has become an essential skill.

9 Necessity!

Trying to get an ISDN line installed in the North East corner of the US isn't as straightforward as it once was. Although officially still available, this is becoming increasingly difficult. In other regions of the world, such as Sweden, ISDN can no longer be obtained as a service. The financial model supporting these legacy synchronous technologies within various Telcos around the globe has evaporated, superseded by IP for the very reasons outlined above. There is also a dwindling knowledge base regarding these technologies within the Telcos which has an obvious effect on service levels, response rates and reliability.

We firmly believe that the Audio over IP revolution is an unstoppable force. The technology is not perfect and may not be a direct replacement for many of the existing technologies, particularly with regards to latencies and delay.

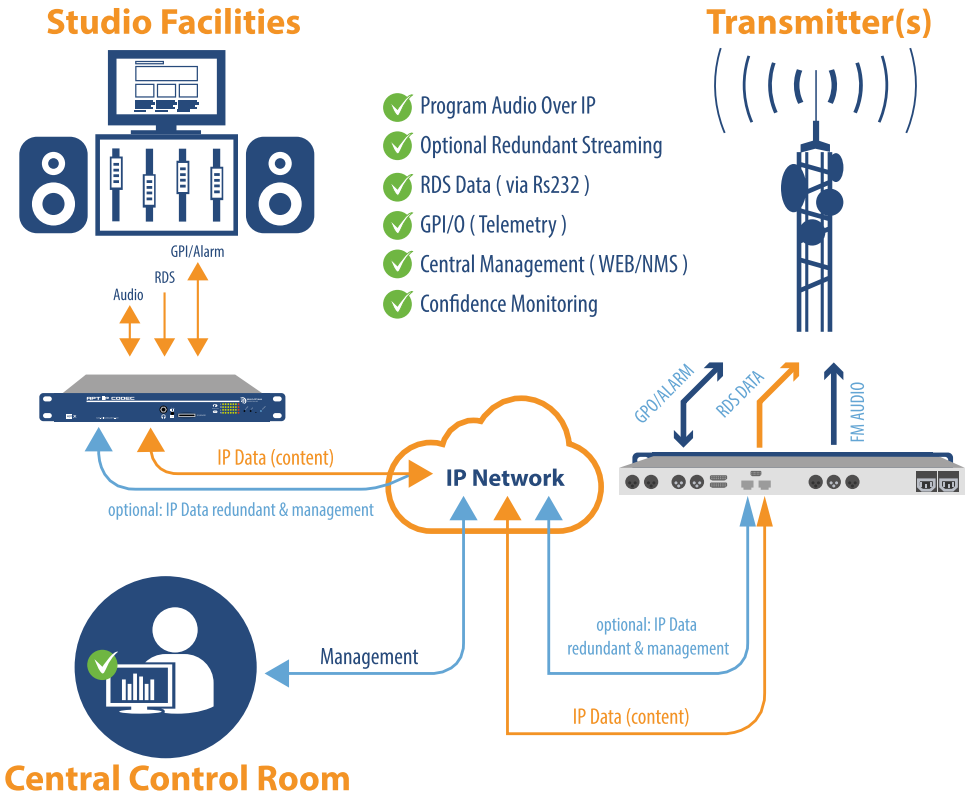
However the many benefits that IP Audio offers makes it an undeniably appealing alternative for those broadcasters who learn how to offset the negative and embrace the advantages listed above!

NEXT…*now that we have explained the benefits and the reasons why broadcasters should migrate to IP let's look at some typical applications in our next section…*

2. IP Audio Applications

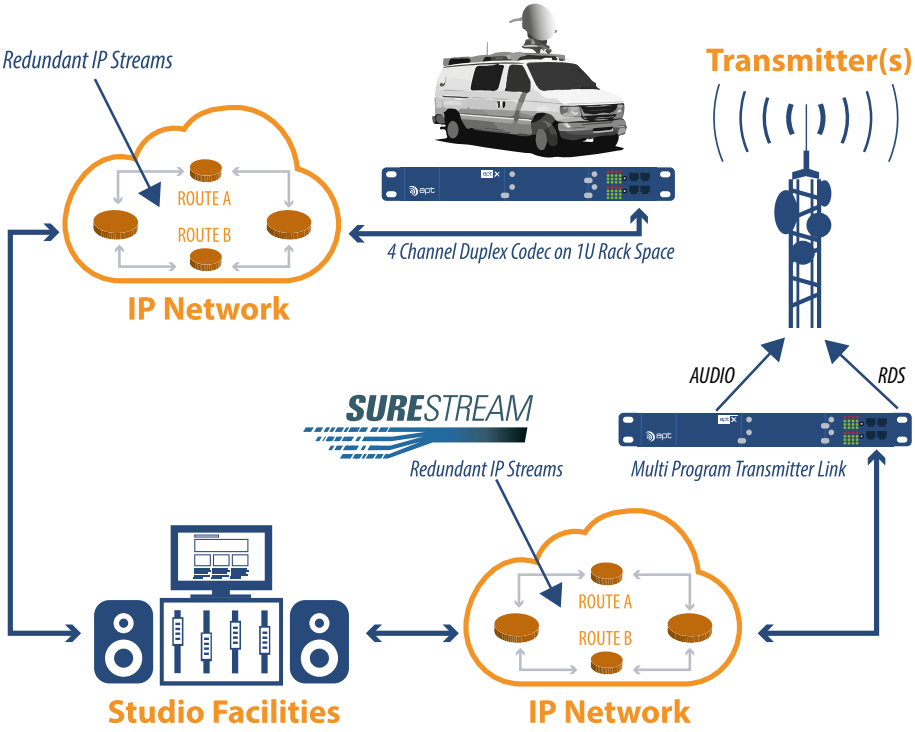
Studio Transmitter Links

One of the most common applications for IP audio in the broadcast chain is the delivery of audio content from the studio to the transmitter site. Most professional codecs will also enable the transport of aux data and telemetry data via GPIO alongside the audio streams. This particular application shows redundant streaming with SureStream technology (see page 69 for more information about redundant streaming.)



Remotes / Outside Broadcasts

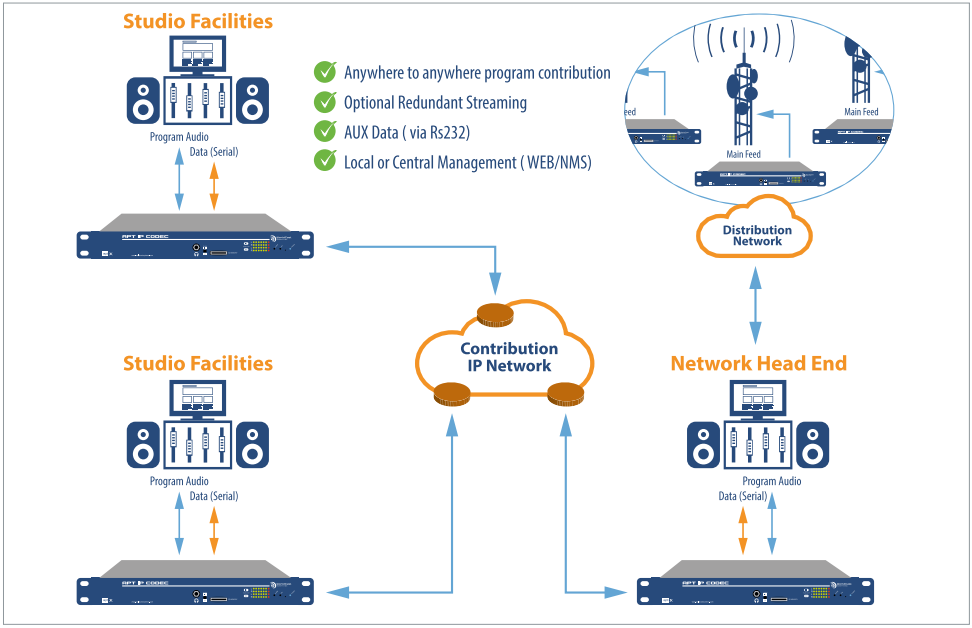
IP networks are raplidly replacing ISDN as the most popular technology for remote or outside broadcast and live program applications. The application shown here depicts a multi-channel live broadcast where both the link between the remote site and the studio and the STL are operating over the public internet using SureStream to protect the integrity of the content.



Audio Contribution & Distribution

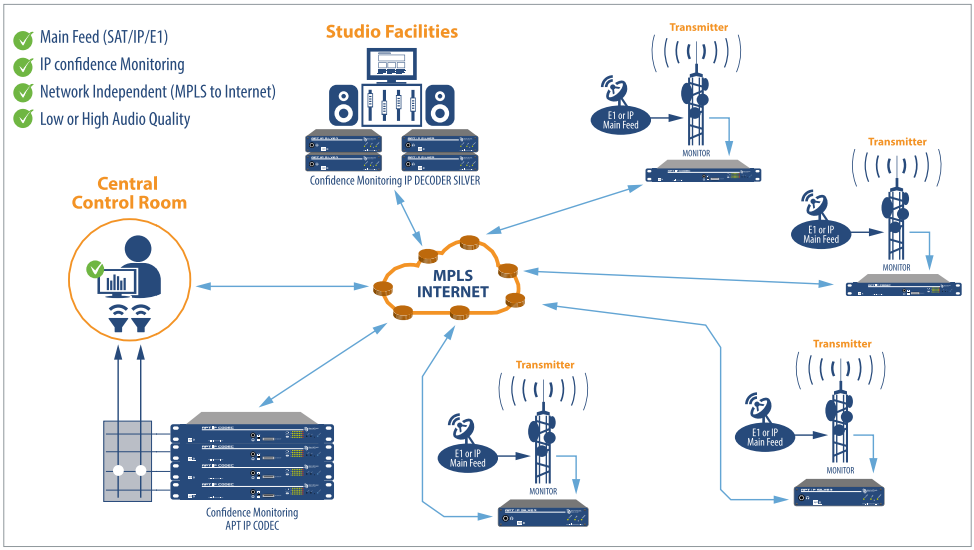
IP Audio Transport enables a highly flexible network wherein multiple channels of high quality audio can be sent between multiple sites. When audio contribution takes place from various regional studios, it is of particular importance that attention is paid to the quality of the audio content so that no degradation takes place before it even begins its journey through the broadcast chain.

IP audio can also be used to distribute audio content to multiple transmitter sites, network head-ends or satellite uplinks. Multicasting or Multiple-Unicasting is often used for distribution (see page 23).



Confidence Monitoring

Confidence Monitoring requires a reliable & cost-effective platform. In the example shown, a mix of stereo APT IP Codecs and separate APT encoder / decoders are used to best match the needs of each location.



NEXT…*now that you have seen some typical applications, in the next section we look at some common considerations for those deploying these Audio over IP applications in the real world...*

3. The Nature of Audio Over IP

1 Packets and Packet Size

One of the reasons IP systems and networks are able to function as they do is the concept of packets. All traffic on an IP network is carried in small packets of data, these packets can be various sizes, but generally not large enough to carry an entire document, song, video clip, or audio recording. The structure of IP dictates that these larger parcels of data be divided and distributed across a number of packets.

Each packet contains a small piece of payload data, but there is another section of the packet that is called the "header". It contains information about error correction, size of the packet, type of data contained, and most importantly, the network address to which that data has been sent (Destination IP Address). The "from" address (Source IP) is also contained in the header information. The packet header is examined and information is by the routers and switches which constitute the routing intelligence on the network and take decisions as to how, when and where to route each packet.

2 Bandwidth,Compression & Compromise

The choices made with regards to audio settings, i.e., the audio algorithm, the audio mode (stereo or mono) and the sample rate will define the data bandwidth required to transport encoded audio over the IP network.
For synchronous connections this actually equals the bandwidth required to transport the compressed or linear audio. But in the IP domain we must add an overhead that is required to packetize the audio data. The figure on page 16 below shows the mandatory overhead (headers and CRCs) of an Ethernet frame for RTP/UDP transmission regardless of the payload transported in an IP packet.

It also shows that an Ethernet packet consists of a number of encapsulations.

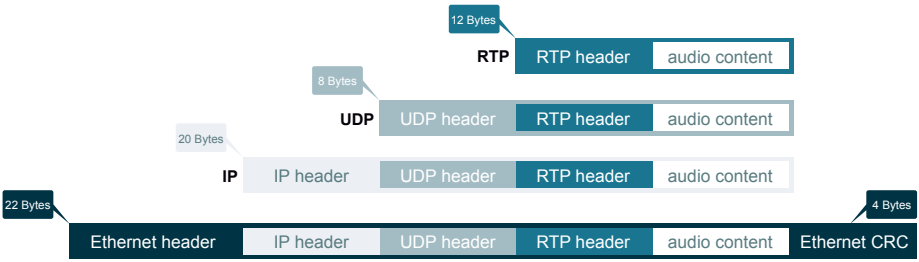
These encapsulations are typical for an RTP/UDP media stream.

While the user can typically control the overall size of their packets, these settings only affect the amount of payload data in each packet – the size of the header remains the same. A smaller packet size will require more packets to transfer the payload from point A to point B.

But for streaming type services such as real-time audio and video, such variations in the delivery delay would be unacceptable. Arriving data must be played out more or less as fast as it arrives and it is likely that some data packets will be lost during the transfer.

One obvious effect of a lost packet is that the data in that packet is gone. In audio terms, it would be a short dropout. In video streaming, it could cause pixilation, or even a freezing of the frame. While choosing a larger packet size will reduce the overall bandwidth requirements and network jitter, it also means that if a packet is dropped, a correspondingly larger amount of payload data is lost.

On the other hand, reducing packet size will reduce packetization delay at the cost of higher bandwidth requirements. Since the header information is a fixed number of bytes per packet, the bandwidth needed to transfer a real-time data stream actually increases as the packet size decreases. Finding the optimum packet size will always be a balance between bandwidth efficiency, network latency and audio quality.



The Ethernet header and sub headers of an Ethernet frame carrying RTP/UDP data

A recommended value for real time transmission is an interval of 4ms. This means one packet contains audio of 4ms (known as p-time) and is sent every 4ms. Depending on the chosen audio format, this 4ms of audio results in a certain payload size.

The table overleaf (see page 17) shows the relation between a packet size in Bytes and p-time (packetization delay) of an unframed ADPCM algorithm (Enhanced apt-X).
The minimum RTP payload depends on the minimum amount of information that an audio algorithm provides.
For linear PCM and all ADPCM algorithms (Eapt-X, G.711, G.722, MICDA etc.) the minimum amount is defined by a PCM sample defined by the sample frequency.

As an example: a PCM sample of FS=48kHz is 20.8µs and for Eapt-X 83.3µs; with this type of algorithm a very small packet size or p-time is achievable (typically ~1ms).

Framed Algorithms

All framed algorithms require additional information about the compression scheme which means they must receive a number of samples before decoding. This number of samples and the accompanying information are encapsulated in algorithm 'frames'. As a recommendation the algorithm frame size defines the smallest amount of information that must be encapsulated in an IP packet and this amount is significantly higher than that of an unframed algorithm.

Audio Data Rate	Payload (RTP) Packet Size Bytes	Eth. frame Size Bytes +66 Bytes)	IP Pkts/Sec	Packet-ization Delay ms	Eth. Data Rate
64 kbps	128	194	62.5	16	97.0 kbps
64 kbps	256	322	31.25	32	80.5 kbps
64 kbps	512	578	15.625	64	72.3 kbps
64 kbps	1280	1346	6.25	160	67.3 kbps
128 kbps	128	194	125	8	194.0 kbps
128 kbps	256	322	62.5	16	161.0 kbps
128 kbps	512	578	31.25	32	144.5 kbps
128 kbps	1280	1346	12.5	80	134.6 kbps
256 kbps	128	194	250	4	388.0 kbps
256 kbps	256	322	125	8	322.0 kbps
256 kbps	512	578	62.5	16	289.0 kbps
256 kbps	1280	1346	25	40	269.2 kbps
384 kbps	128	194	375	2.7	582.0 kbps
384 kbps	256	322	187.5	5.3	483.0 kbps
384 kbps	512	578	93.75	10.7	433.5 kbps
384 kbps	1280	1346	37.5	26.7	403.8kbps
576 kbps	128	194	562.5	1.8	873.0 kbps
576 kbps	256	322	281.25	3.6	724.5 kbps
576 kbps	512	578	140.625	7.1	650.3 kbps
576 kbps	1280	1346	56.25	17.8	605.7 kbps

FIG. A Relation between audio payload, packet size, p-time (packetization delay) and the Ethernet data rate.

3 Audio Algorithms

When choosing the best format of sending audio down an IP link, restrictions in available bandwidth, minimum latency and the required audio quality will influence the choice of a suitable audio format or audio compression algorithm. There are several main types of formats and algorithms:

Uncompressed digital Audio

- Linear PCM 16/20/24Bit
- AES transparent (linear PCM in an AES frame)

Digital Companding Systems

- ITU J.41/J.42
- ITU J.57
- G.711

ADPCM based Algorithms (Adaptive Differential Pulse Code Modulation)

- G.722
- Apt-X, Enhanced apt-X
- 4SB ADPCM

Perceptual Algorithms

- All derivatives of MPEG algorithms
- OPUS

Perceptual based algorithms use psycho-acoustic based principles which analyze audio content and determine what is audible to the human ear. The algorithm will remove all inaudible content and is therefore, by definition, "lossy". However, the compression ratios that can be achieved with perceptual algorithms are impressive and much higher than any other method. The downside of this approach is that using multiple passes of encoding/decoding cycles will introduce artefacts into the content and lead to a relatively high processing delay.

ADPCM algorithms offer a more robust signal quality and very low latency given their gentler, non-destructive approach to coding. Therefore ADPCM codecs are often used in contribution applications where the high signal quality and the low delay are of great importance. The compression ratio achievable with ADPCM is comparatively low. The apt-X and 4SB ADPCM algorithms achieve a 4:1 ratio.

A digital companding system is, from today's point of view, a legacy coding technology, but can still be found in broadcast contribution as well as in distribution applications. The principle is based on dynamic companding where a high signal sample is digitized on a lower bit resolution than the low signal samples.

The idea is to minimize quantization noise on low level content and maintaining a defined bitrate on the transmission chain. The main digital companding systems are ITU J.57, a 20kHz format mainly used in contribution applications and J.41, restricted to a bandwidth of 15kHz purely for FM transmitter feeds. The quality achieved on both formats is very high and the delay is very low.

Companding systems were once the highest quality standard but nowadays these systems are almost completely replaced by ADPCM or linear PCM formats. Today, uncompressed audio transmission is becoming increasingly prevalent. Due to the ever-increasing bandwidth available on site-to-site links, linear PCM or even transparent AES/EBU is now a viable alternative. With linear PCM, maximum audio quality is guaranteed and low latency becomes a concern purely for those designing the network architecture.

For the last 20 years, the development of coding algorithms has been focusing on the optimization of parameters such as bitrate, quality, encoding/decoding, latency and compatibility and we are currently in a situation where an optimum solution can be found for almost all broadcast applications.

The table below characterizes the most common formats and algorithms used in broadcast applications. The bit rates given are examples; more bit rates are possible per algorithm and the list is not exhaustive.

New Audio Formats and Algorithms

Opus

is a quite new codec algorithm and utilizes two established codec approaches. The combination of a modified version of SILK (based on a voice codec from Skype) and an extended version of CELT results in the very flexible OPUS audio codec.

Algorithm Format (stereo)	Bandwidth	Data Rate kbps	Latency average	Application
Linear PCM 16Bit	22kHz	1,536	Very low	Contribution
Linear PCM 20Bit	22kHz	1,920	Very low	Contribution
Linear PCM 24Bit	22kHz	2,304	Very low	highest quality link
Eapt-X 16Bit1	22kHz	64-384	Very low	Distribution
Eapt-X 24Bit	22kHz	192-578	Very low	Contribution
G.711	3,400Hz	64	Very low	Speech
G.722	7,000Hz	64	Very low	HD voice
ITU J.41	15kkHz	384	~5ms	Distribution
ITU J.57	20kHz	1,920	~5ms	Contribution
MPEG1 LII	Up to 20kHz	64-384	~50ms	Distribution
MPEG1 LIII (MP3)	up to 20kHz	64-384	~100ms	Distribution
MPEG2 LII	Up to 20kHz	64/128	~90ms	Distribution
MPEG2/4 LD2	Up to 20kHz	128-256	~30ms	Distribution
MPEG2/4 LC3	Up to 20kHz	32-384	~50ms	Distribution
MPEG2/4 ELD4	Up to 20kHz	128-256	~20ms	Distribution

Relationship between audio payload, packet size, p-time (packetization delay) and the Ethernet data rate.

Celt is a royalty-free lossy audio compression and was initially developed and maintained by the Xiph. Org Foundation. CELT has now been merged into OPUS and abandoned as stand-alone codec. SILK and CELT work in a hybrid mode with seamless mode switching, where CELT is most efficient on full-band audio (FS 48kHz) while SILK (modified) is very good at narrowband and wideband speech up to approx. 32kbps.
The main attributes of OPUS are high scalability and low latency. Due to its scalability, OPUS is suitable for almost all applications from VoIP to high quality video conferencing, or from low bit rate music streaming to a low delay broadcast application. OPUS can even be the format of choice for high quality music performance.

Key characteristics:

- Sampling Rate: 8 – 48kHz
- Bit rates: 6 – 510kbps
- Frame size: 2.5 – 20ms
- Mono and stereo support
- Speech and music support
- Seamless switching between all of the above
- Low delay in the range of 20ms

The OPUS codec is already integrated into modern Web browsers like Mozilla Firefox, Opera and Google Chrome (others will follow soon).

AES67

All the audio algorithms we have discussed so far are suitable for audio networking in a WAN (Wide Area Network) environment. Under these schemes, the bitrate of an audio stream can be modified in accordance with the available bandwidth on the WAN.

AES67 is a recently developed standard to achieve interoperability for audio networking in the LAN domain only. In terms of applications therefore, it allows real-time streaming in broadcast and production facilities between audio equipment providing an AES67 interface.

The standard outlines the format of multi-channel audio transportation (streaming) over IP networks - essentially multi-channel audio on a single RJ45 connector. It does not allow any audio compression or any other bitrate adaption with the exception of defining a definitive number of audio channels but it incorporates synchronization mechanisms based on the precision time protocol (PTPv2 IEEE 1588). As the technology gains in popularity, audio codec manufacturers will provide AES67 interfaces alongside current analog and AES-3 connectors.

NEXT…*hopefully this section has provided an understanding of many of the key considerations related to Audio over IP. In the next section we will examine the array of different network choices on which to deploy your AOIP network. We also examine some general considerations and issues you may encounter along the way…*

4. About IP Networks

Types of IP Networks

IP networks were designed to transport non-time sensitive data from point A to point B within an acceptable timeframe. Should data get lost or delayed, files can be re-sent and webpages refreshed. However, this is not possible in a broadcast environment where reliable, real-time audio transport is an imperative.

In order to deliver successful audio over IP broadcasts, engineers need to familiarize themselves with the nature and inherent characteristics of packetized networks.

Service providers offer broadcasters a variety of different options for IP audio delivery. These range from dedicated links with a guaranteed Quality of Service to the open internet or contended ADSL links. We will examine each option in turn and evaluate their usefulness to the broadcaster.

A key concept here is that no network is perfect. Even closed and monitored systems like Dedicated links, microwave links and MPLS links can be sources of packet loss and jitter, which can negatively affect the audio quality.

Dedicated IP Links

Professional studio transmitter links and inter-studio networks require a reliability and robustness that is typically not available on unmanaged public networks. The mission-critical nature necessitates a guaranteed service level that will ensure the uninterrupted flow of packets from the sender to the receiver with minimum delay and no loss of audio quality.

For these applications, some service providers will offer some form of dedicated IP connection offering 'always on' access and, a choice of failsafe options to ensure mission critical connectivity. This service should be uncontended with no bandwidth sharing to avoid disruption of on-air content. If this is not possible, the broadcaster should request the lowest contention ratio possible.

Dedicated IP access service is typically backed by a Service Level Agreement (SLA) and traffic priority mechanism, such as Quality of Service (QoS). Without such an agreement, a broadcaster will have no control over IP network conditions and therefore no control over the quality of the audio emanating from that network.

MPLS Links

Offering one of the highest levels of service possible with IP, Multi-protocol Label Switching (MPLS) networks are increasingly replacing leased lines as the transport mechanism of choice for STLs and SSLs. The technology offers many of the benefits of leased lines in that it is a connection-oriented service and so has the ability to support bandwidth reservation and service guarantees. In addition, it is also complementary to IP transfer and therefore offers the cost, flexibility and efficiency benefits of IP audio networking.

MPLS assigns each network packet with short (20bit) labels that describe the path which that packet should take. In comparison to a traditional IP network where individual routers make independent routing decisions, MPLS traffic is analyzed upon entry to the MPLS cloud and assigned a 'label' which dictates its path throughout the network.

Without the need for each router to look up the address of the next node, MPLS offers a faster, more efficient service than a standard IP connection. Additional information for traffic class of service (priority) can also be included in the MPLS label to ensure prioritization of critical, time-sensitive content. Overall MPLS networks offer an attractive solution for broadcast networks. They are typically available at a lower cost than traditional synchronous leased lines with a higher performance than conventional IP links. They enable scalable and flexible networking, support Quality of Service and will integrate with many transport methods including IP, ATM and Frame Relay.

Wireless IP Links

Improvements in the scale and capabilities of Wireless and microwave IP networks make these a solid option for broadcasters. Depending on the class of microwave service deployed, IP data can be linked in both directions at respectable speeds (100 mbps or more). There are two classes of microwave IP, in general. The "unlicensed" class operates in the 5.8 GHz band and the 2.4 GHz band amongst others. While inexpensive and useful for certain applications, it offers no protection from interference. Licensed microwave IP operates at 6, 11, 18, and 23 GHz, with even faster speeds and protection against interference. Even though a microwave IP link is essentially a "closed" system, it can still suffer from packet loss and jitter.

Satellite IP

IP links via satellite are the only option for some broadcasters, with sites so remote that even ADSL or microwave IP links can not be used. The primary challenges of using satellite IP are latency (the amount of time it takes a packet of data to travel from one end of the link to the other) and expense. Typical latency on a satellite IP link can average 2 seconds or more. Satellite is generally the most expensive bandwidth, which can be a significant factor when planning a link that will carry high-quality audio 24/7.

Public Internet

As we have noted, it is challenging to utilize unmanaged networks such as the open Internet for professional broadcasting applications, whether the connection is via cable, ADSL or fiber. However, technology has been developed that can virtually eliminate the negative effects of using public Internet for delivery of real-time broadcast quality audio.

The Internet can also be used for remote broadcasts and it is possible to achieve high quality real time audio transfer using contended IP links. Utilizing the public internet means that the broadcaster is more exposed to the risks associated with IP links and, therefore, extra care needs to be taken to eliminate any risks with regards to the codec equipment and technology employed. As a minimum, the codec should be DSP-based for rock solid reliability and offer remote configuration and control over IP. In addition, the following should be ensured:

- Auto Re-connecting Codec - The codec used must enable fast re-connection if the link is dropped. Some manufacturers' codecs require a manual reboot at both ends to re-establish the connection.

- Low Delay, ADPCM Coding - Perceptual coding technologies such as MPEG Layer 2, AAC etc are frame-based and therefore require a minimum of one algorithm frame to be buffered before compression is applied. If the link is dropped due to network outages, this buffering will introduce additional delay into the audio stream. ADPCM algorithms encode and decode 'on the fly' enabling instant audio immediately upon reconnection. They also enable flexible packet sizes which can minimize the effects of dropped packets on the audio stream.

- IP Packet Resequencer - In contended networks such as the public internet, there is a higher likelihood that packets will be delivered out of sequence. Codecs that have been developed for professional use should offer resequencing technology to ensure that all packets received are played out in order, thereby minimising audio glitches. An IP packet resequencer will work within the receive buffer to re-order the packets according to their RTP sequence number.

Redundant Streaming – APTs Sure Stream technology (see page 69) delivers multiple streams of audio from source to destination, so that any packet drops or Loss of Connection events that affect one stream can be corrected using the data from the redundant streams. This solution does require more IP bandwidth at each end, but makes all networks more reliable, when using the public Internet. Inexpensive bandwidth such as ADSL or cable can now reliably and permanently replace synchronous links such as E1, T1 and ISDN with no loss of audio quality or reliability.

Types of Connections

Due to the highly flexible nature of IP, networks can be utilized in many ways. One of the more significant advantages is the capability of sending data from one host to many others simultaneously.

A single connection from one host to one other host is called a **Unicast**, it is the most basic type of permanent streaming connection.

Individual data links can also be established and real-time data streamed from one host to multiple destinations, this is called a **Multiple Unicast**. Each is a separate point-to-point link and requires its own bandwidth from the common host. These types of connections are generally simplex, with data moving only from the host out to the multiple locations.

There is also a special and very unique configuration called **Multicast**. In a multicast, a single stream of content is generated by a host and sent to an IP address that is in a unique class. The data is then duplicated in the network hardware and delivered to any other hosts that have requested to receive the stream from that multicast address.

This has an advantage of requiring less bandwidth from the source host to get the content to multiple locations, but it requires specific network hardware and configurations, and can rarely be used outside of a private network. The Internet does not support multicasting, in general.

The Components of an IP Network

There are three pieces of information that are essential for each host on a network, as they define the scope of the local network structure, and how hosts on that local network can connect to the wider networks and Internet. These three elements are defined below:

IP Address

An IP address consists of 4 'octets', separated by periods. An octet is 8 bits of information, so each octet can be anywhere from 0 to 255 (in decimal), giving us the familiar xxx. xxx.xxx.xxx format. Each host on any given network must have a unique IP address. Certain groups of IP addresses have been designated as non-routable, in that those addresses cannot be reached from external network segments. Common non-routable groups are 192.168.xxx.xxx and 10.0.xxx.xxx. In order for these devices to be able to access outside networks, they must communicate through the gateway on their network.

Gateway

The gateway is the bridge between one network and the wider networks beyond. When you log on to a computer and ask it to connect to the Internet, the computer contacts the gateway and the gateway forwards the request on to the outside network, and routes the returning information back to the local host. This typically involves port forwarding and Network Address Translation (NAT) which are defined in more detail on pages 41. The gateway hardware is typically a router, and may also include a firewall, to prevent unauthorized traffic from the outside network reaching the IP addresses on the local area network (LAN).

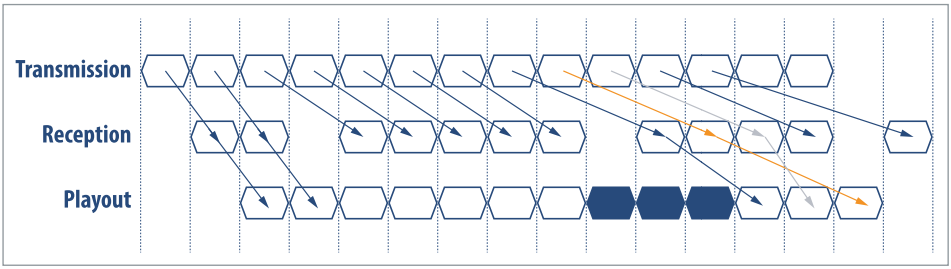
Mask

The mask is like a fence surrounding the local network, and determines what IP addresses a local host can reach directly, and what IP addresses must be contacted through the gateway. For example, with a common local IP address of 92.168.1.23 and a typical mask of 255.255.255.0, any IP address that matches the first three octets of the host address (192.168.1.x) is considered a local IP. A request to contact an address outside that fence – for example 192.168.2.xxx – will be sent to the gateway.

Network Imperfection

1 Dealing with Jitter

It is a characteristic of packet switched networks that any packet can take any route from source to destination, thus it is inevitable that some of those packets will arrive out of sequence. All streaming codecs have a buffer and other technologies to store and replay the packets in their proper order, but most of those solutions have limits. Jitter occurs when packets arrive before or after their predicted arrival time and the receiving codec is unable to achieve real-time playout.



Network Jitter Effects

The larger and more complex the network structure, the more susceptible the data stream will be to jitter, with the public Internet being a most difficult environment in terms of jitter severity. The above diagram shows the effect of network jitter on the reception of audio and its subsequent playout through an audio system. The buffer depth will usually be set in milliseconds but, for the purposes of this example, it is set to a two packet buffer. Provided the network jitter is low, the system is unaffected and plays out the packets received in sequence.

However, should jitter increase beyond the pre-determined buffer, packets which arrive after the determined playout time will be dropped, resulting in corrupted audio. Again a trade-off is necessary, this time between the size of the jitter buffer and the additional playout delay introduced. Setting a large buffer to minimize the effects of jitter may substantially increase the overall network delay.

2 Dealing with Delay

All networks have transport latency due to the natural laws of physics. Transporting an electronic signal through any medium will take a finite amount of time that cannot be removed.
In an IP network, added to the standard transmission delay is the delay necessary for packetizing the audio data, so best case latency on an IP network will typically be at least 10-30 milliseconds. As noted previously, packet size and jitter buffering will also have an effect on the size of the delay.

The latency figure quoted represents the inherent latency throughout the network as the data passes through switches, routers, etc. and does not include audio compression delay nor sample frequency effects. Any coding delay resulting from the use of compression will add directly to the existing latency of the system. And of course on a wider area network (WAN) or public Internet connections, delay can grow into hundreds of milliseconds. Plus, the latency can vary widely, as the data packets flow across the various networks and links. When using a standard IP connection, the only way to compensate for this large and variable latency factor is to establish a receive buffer of sufficient size.

The choice of audio compression algorithm is also important in determining the end-to-end latency of the system. Linear audio or low delay compression coding techniques such as Enhanced apt-X will normally be selected for real- time audio over IP applications. With the expansion of digital audio broadcasts, the latency of the delivery link has become a less critical factor.

3 Packet Loss

Depending on the quality of an IP link and the bandwidth available, packet-based systems can be susceptible to dropped packets. As we learnt in the previous chapter, the resultant loss in audio will relate directly to the size of the lost packets, the number of packets lost and the compression ratio used. With frame-based algorithms such as MPEG, the loss of any packet in a frame requires the frame to be discarded. Therefore, using small packet sizes in conjuction with these coding technologies will not bring any benefit or lessen the effects of packet loss.

The Enhanced apt-X algorithm requires no frame buffering and offers greater flexibility in packet size selection. This reduces the susceptibility of an audio stream to the consequences of packet loss. Packet sizes with durations down to 1 msec are easily achieved with Enhanced apt-X.

Algorithm	Mode	Bit Rate	Packet Size (Bytes)	No Of Audio Samples	Audio Lost
MPEG Layer 2	16 Bit Stereo	256 Kbps	768	2304	24ms
Enhanced apt-X	16 Bit Stereo	256 Kbps	512	64	16ms
Enhanced apt-X	16 Bit Stereo	256 Kbps	64	8	2ms

Table showing how choice of compression algorithm affects packet loss

NEXT…*you should now have an idea of the challenges you could face when implementing an AOIP solution. In the next section we will look at the techniques used to counter some of these challenges or imperfections inherent to many IP networks…*

5. Overcoming Imperfections

With such huge benefits to be gained from migration towards an Audio over IP based architecture, it is not surprising that R&D departments, codec designers and engineers worldwide have dedicated many years to trying to find solutions to overcome the disadvantages and imperfections of IP audio in order to properly take advantage of its cost and flexibility.

Below, we outline some of the methods that have been explored and adopted with varying degrees of success.

a Concealment

Various methods can be used to conceal lost packets in the final reproduction of the audio. They range from simple repetition of the last good packet received, to silence/noise injection or interpolation and retransmission. All have an impact on the reproduced audio.

In listening tests the injection of silence produced unacceptable breaks in the audio that led to a level of incoherence. The use of white noise improved the intelligibility of the reproduced audio but was again noticeable. The use of repetition of the last known good frame produced more favorable results.

The use of interpolation/pattern matching/waveform substitution to conceal the loss of packets is possible but the benefits versus complexity are governed by a law of diminishing returns. The results of these techniques are all governed by subjective improvements in audio quality and are also subject to the amount of audio lost that is being concealed or repaired.
None of these concealment options produce an easily workable solution and it is the generally accepted view that a better approach is to minimise the packet loss rather than trying to disguise it.

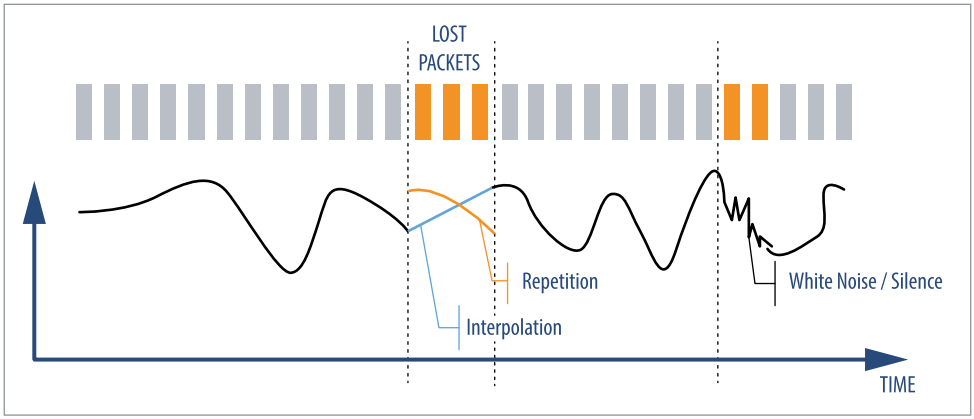
b Forward Error Correction

Forward Error Correction (FEC) is a means by which lost packets can be reconstructed for playout. The simplest form of FEC adds redundant data based on the XOR of the data in each packet with at least one or two other packets (Figure overleaf). The resultant FEC packet is added to the transmission and used in conjunction with the data received to correct any errors present and reconstruct the audio stream.

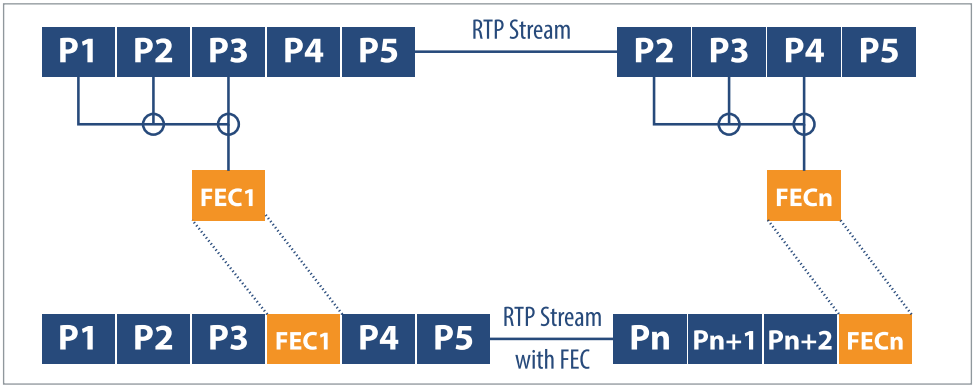
While this basic form of FEC works well for small amounts of random packet loss, it cannot deal with the more common occurrence of burst packet loss (ie several adjacent packets lost at once). In order to deal with burst errors, a more complex FEC scheme such as that shown on page 29 is required. This FEC scheme calculates in two dimensions which provides more data to the recovery engine.

As you can see from the following illustrations, any form of FEC will add substantial overhead to the audio stream and, in some cases the transmission bandwidth is effectively doubled. In networks where bandwidth limitation or congestion is a problem, using FEC is not a viable option. In addition to the bandwidth issues it introduces, generating FEC at the encoder is processor intensive and will introduce even more latency.

The complexity of the FEC, the packet size and compression ratio used are all factors which influence the resulting delay. For example a two by two FEC requires the buffering of four packets.
Given our earlier calculations concerning the amount of audio in an MPEG L2 packet, this equates to 96ms. A two by two FEC will only protect against a small burst error and the more realistic five by five FEC (as shown in the figure below) will require 25 packet buffering which, using the same calculations, is equivalent to 600ms delay.



Packet Loss concealment

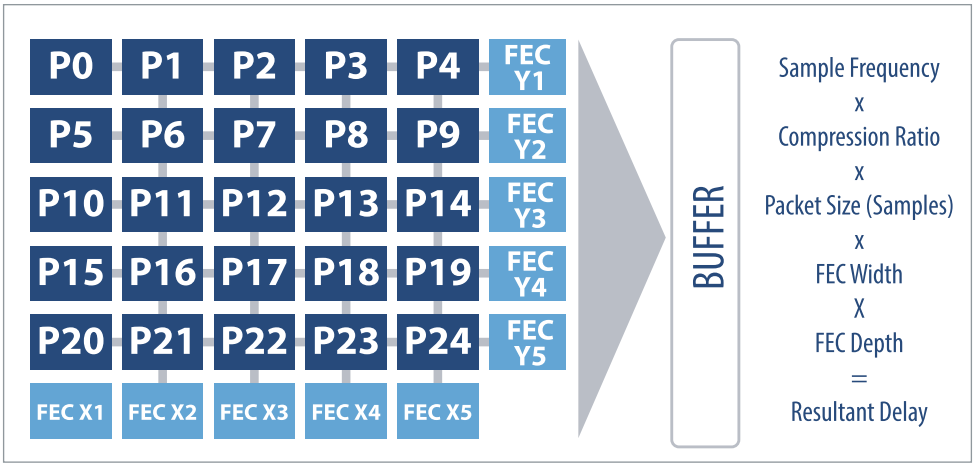


A Basic FEC Scheme

Recovery on the decoder-side is also processor intensive. The process of amassing the required block of packets, determining

the location of the lost packets and resolving them one by one can be a lengthy and complex procedure.

As with concealment, the use of FEC can cause as many, if not more, problems than it solves. It can go some way to overcome the inadequacies of an IP based transport mechanism but at a cost of additional delay, complexity, bandwidth and processing overhead.



A Two Dimensional FEC Scheme

C Quality of Service

In order to improve upon the basic transport service offered by IP networks, known as "Best Effort Service", many service providers will offer mechanisms to guarantee the delivery of time-sensitive content. An audio stream on an STL will require minimal interruptions to packet flow while data may only require that it reaches its destination within a reasonable timeframe. Quality of Service (QoS) was designed to provide a mechanism which allocates different levels of service or priority based on the importance and time-sensitivity of the traffic.

There are two main methods for the improvement of link quality: RSVP and DiffServ.

- **RSVP** (Resource reSerVation Protocol) is more complex and involves the reservation and relinquishing of required resources throughout the network.
- **DiffServ** (Differentiated Services) on the other hand offers a traffic classification framework that evaluates the priority of network traffic on a "per hop" basis. Using Diffserv, each packet is classified and awarded a DSCP (Diff Serv Code Point) value that is evaluated by the network and prioritized accordingly.

This scheme can be very effective on internal networks where the user can control and select routers and other network hardware that support the DiffServ codes. However, the public Internet – even if it is a private VPN or WAN link set up across the public Internet – does not support QoS in any form that could be considered robust enough to support critical real-time audio links.

d Service Level Agreements

Some Telco or other service providers may offer an SLA for an IP link typically guaranteeing uptime in percentage terms. This percentage can be reconciled to criteria such as lost packets and actual down time on the link.

Typically an SLA will consist of the following parameters:

- The performance which the service provider will guarantee for the client's traffic. This will usually include the delay across the network, maximum jitter and packet loss levels.
- A guaranteed availability of the service which for broadcast applications should be 99.999% or higher.
- The scope of the service i.e the specific routers between which the SLA prevails.
- For professional STLs and audio backhaul, the emphasis should be on ways to minimize packet loss. Implementing methods to conceal or correct errors is an unnecessary distraction to the main aim of ensuring reliable, robust audio delivery over an IP link.
- The bandwidth profile of the stream delivered to the service provider
- Performance monitoring procedures and expected levels of reporting
- Support and troubleshooting procedures including time-frame for response and resolution and consequences for non-compliance
- The administrative/legal part defining processes for requesting and cancelling certain services.

Generally the SLA will specify how the customer is to monitor performance under the SLA, often via an online tool.

If performance fails to meet the figures specified, the SLA also covers the formulas to determine penalties to the carrier (most often in the form of credits to the customer, not refunds). An SLA may only be available to the broadcaster with certain revenue commitments (contract amount) or periods (contract duration). And of course even the most stringent SLA cannot protect against lost packets, it can only compensate for loss of services after the fact.

e Alternative Connection

Even with all necessary due diligence applied in the selection of the IP Network & Service Provider, there is still the possibility of a major outage on the network. This can cause the broadcaster to be off-air unless they have a backup solution in place. A primary IP link can be backed up either by a secondary IP link supplied by a different service provider, a microwave IP link or by other means.

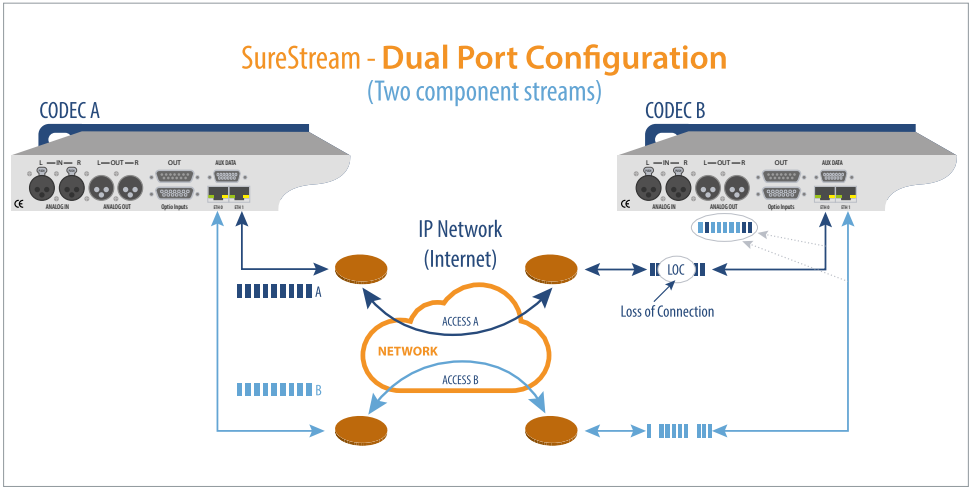
Professional audio codecs will provide the ability to trigger the backup from the primary IP link to the secondary link using a number of different criteria such as silence on the audio output of a specific audio module or a defined threshold in the Performance Monitoring log.

f Redundant Streaming (SureStream)

More advanced codecs and technology can generate and deliver multiple redundant audio streams from one source to one or many destinations. The data in each stream is identical, and by routing these multiple streams across divergent network paths – particularly by using multiple ISPs at each end of the link – it is possible to provide a high level of confidence in packet delivery, without the audible artifacts of "switching" from one link to the other.

This "always-on" redundancy provides the ideal solution for long term, highly reliable real-time audio links over any type of packetized network. Microwave, DSL, Satellite, cable Internet – any kind of network bandwidth can be used.

The only sacrifices are buffering (necessary for all packetized network streaming) and bandwidth. Since each redundant stream will occupy its own bandwidth on the network,



sending redundant streams means a greater network speed is required. However, with the Enhanced apt-X algorithm, multiple redundant streams can be sent across almost any network link.

"Always on" redundant streaming provides the best possible performance for streaming audio over imperfect networks. It applies the strength of a network – copious bandwidth and self-healing path diversity – to solve the problems inherent in that same network.

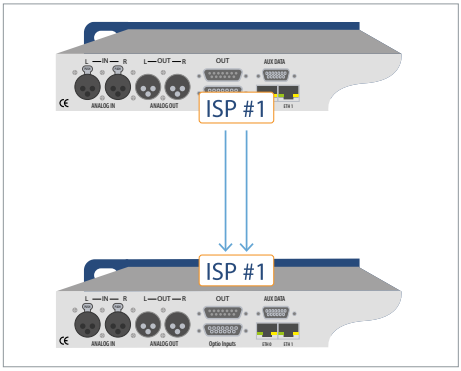
Packet losses can be almost completely eliminated, and with multiple network paths at each end, even Loss of Connection events can have zero impact on the payload audio. If a packet is missing from one of the "contributing" streams, it is replaced by its twin from another stream, before that audio leaves the buffer.

There are no glitches, pops or clicks, no variations in audio quality, and no changes in the playout timing, which is critical for contribution networks and others that need to meet a precise time window with their audio.

In terms of network architecture, redundant streaming can be deployed in several configurations.

GOOD: Redundant streaming on a single network connection on each end.

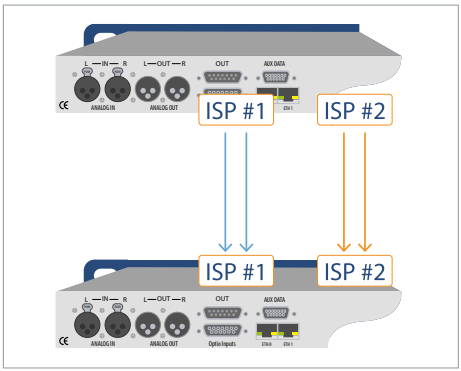
This configuration provides good protection against packet loss, but a single connection is still vulnerable to LoC events and "burst" losses, where many packets are dropped in a short amount of time. Bandwidth permitting, you could send three or more streams on that single connection and improve performance somewhat, but burst losses and LoC events could still potentially affect the audio.



GOOD

BETTER: Dual parallel network paths.

This configuration helps to eliminate any single point of failure. It greatly reduces the chances of an LoC event affecting the audio, and also makes a big performance improvement against packet loss, even burst losses. Common paths used in these types of deployments include MPLS networks, WANs, microwave IP transport, DSL connections, 4G, cable, fiber, and even satellite.

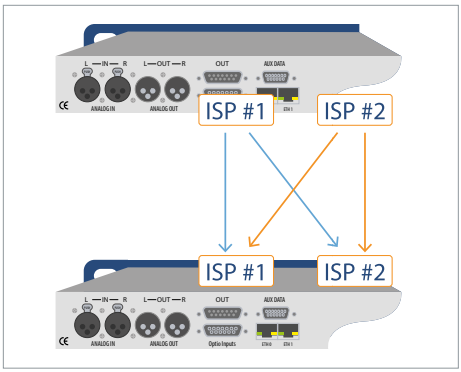


BETTER

BEST: Dual crossed parallel network paths

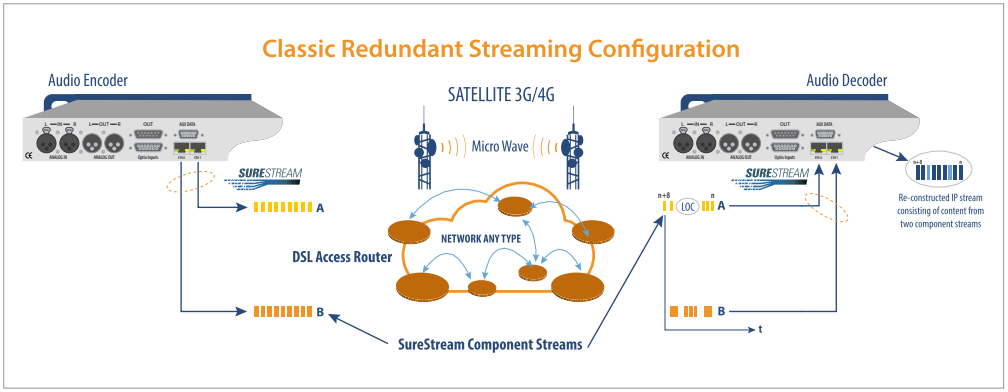
Where network architecture permits, one or more contributing streams can be sent from each of the origination networks to each of the network ports on the receive end. This configuration is the most robust against any kind of network interruption. Even if a network connection is completely lost, there will still be redundant streams using all of the functioning ports.

Any configuration that uses dual network paths will be extremely robust.



BEST

Long term field testing of SureStream (APTs redundant streaming technology) has shown performance superior to T1 and ISDN, up to 99.999999% and greater reliability of packet delivery, on open public Internet connections, using basic DSL providers on each end.

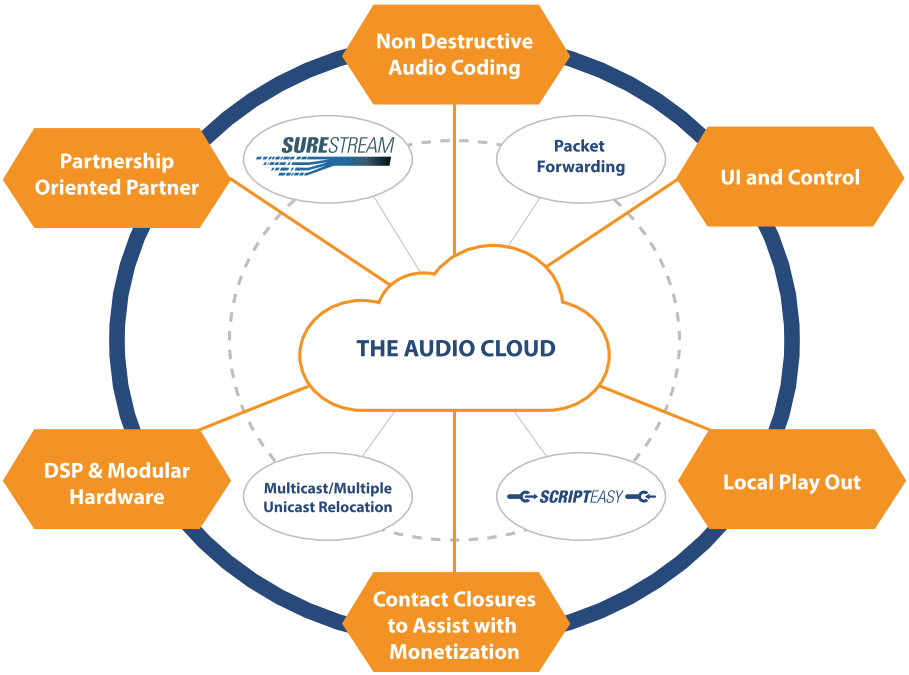


Advantages of Redundant Streaming

Redundant streaming has several clear advantages that make it the best current solution for reliable delivery of audio and other streaming content over the public Internet.

- Redundant Streaming technology is content agnostic
- Redundant streaming is path agnostic
- Redundant streaming offers "always on redundancy" i.e. there are no primary and backup links – no glitches or "switching" from one link to another
- Redundant streaming is totally scalable in cost and technology
- Redundant streaming is applicable to almost all broadcast applications, STL, SSL, Remotes (ISDN Replacement)
- Key benefits over other approaches are:

    * Zero interruptions to service
    * Audio quality consistent
    * Audio delay consistent



The Audio Cloud - "Ultimate Resilience"

The "Audio Cloud" is a fresh concept in broadcast that is allowing the broadcaster and generically the distributor of audio content to realize an architecture that is inherently redundant and self-governing in terms of audio routing and backup.

Ultimately te aim of the "Audio Cloud" is to allow the broadcaster to deliver audio from point A to B or indeed from point A to B to Z as cost effectively as possible with the greatest degree of reliability and the least degree of user intervention. With its similarity to the ring topolgy and drop and insert capabilities provided by T1/E1 networks, the audio cloud concept further increases broadcasters' opportunities to migrate away from traditional broadcast transport infrastructures and Satellite distribution and look at much more cost effective and widely available bandwidth. Whether implemented fully or in part, it represents a solution for all broadcast applications from STL to remotes and from contribution to distribution.

There are four main components of the audio cloud:

- Redundant Streaming
- Distributed Intelligence
- Packet Forwarding
- Multicast / Multiple Unicast Relocation.

The components can be used in combination or selected a la carte to create the audio cloud suited to the broadcasters' application, budget and IP network availability.

Redundant Streaming

Already covered in detail above, this is the core on which any audio cloud is built. This is the ability to stream multiple copies of the same audio packet over divergent networks to protect against packet drop or loss of connections.

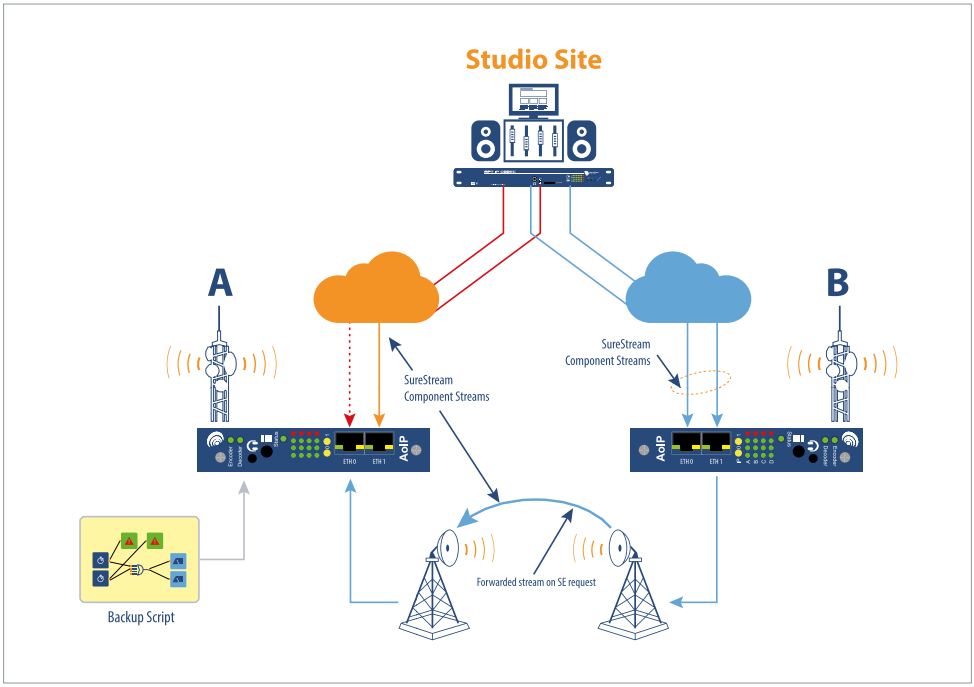
Distributed Intelligence

In order to manage a multi-site audio network, and specifically the performance of the units located in the Audio Cloud, some form of intelligent control is required. The intelligence will draw information from a combination of inputs in the form of contact closures, alarms and measured parameters and use this information to make decisions that will determine how to route the audio, what audio profile to be used and what action should be taken in the event of component stream failures.
An intelligent system is capable of automatic actions both scheduled, such as local content insertion from a preloaded schedule, and unscheduled, such as audio failover to a backup system. The "Intelligence" will therefore continuously examine events and logs and then make associated decisions based on the data received to make the cloud function and self-heal with limited user intervention. It also provides essential reporting and alarming functions that can be relayed to the engineer by email, SMS or DTMF notification.

In contrast to a centralized management system, if this intelligence can live on the audio codec itself, the intelligence is then distributed throughout the network, ensuring that no single point of failure exists. Each codec has its own brain and is able to make decisions independently of the other audio codecs within the cloud. Distributed Intelligence acts as the self-governing, fault-reactive and automated controller of all the audio codecs within the cloud.
In the case of APT IP Codecs, this distributed intelligence comes courtesy of ScriptEasy, a technology developed initially for the Audemat range of facility remote control and telemetry units. As well as making decisions on everything, ScriptEasy is also able to send notifications to the relevant personnel when a predefined scripting action has occurred or some other network event (planned or unplanned) has occurred.
In the event that a broadcaster moves away from a managed service or satellite distribution network provided by a Telco, Distributed Intelligence effectively replaces the NOC (Network operation Centre) that the Telco would have used to monitor and make corrective actions on their networks.

Packet Forwarding

The concept of packet forwarding is very similar to the concept of drop and insert in the E1/T1 (SDH/SONET) Synchronous world. Packet forwarding over IP is essentially the ability to make any decode site on the network also a node capable of supplying other decoders with the audio packets on either a primary or on an automated backup basis. This allows the broadcaster to have multiple encoders as potential encode sources thereby avoiding a single point of failure. The single point of failure could be an actual hardware encoder failure or a catastrophic failure in both network points at the origination point of the encoder. I say specifically the "origination point of the encoder" as, if the broadcaster is using the core Redundant Streaming technology, then a total failure can't happen anywhere on the network!
This ability is inherently useful in building the self-healing audio cloud. In the event of a network failure that leads to loss of the contributory stream, the distributed intelligence element would re-route the packets and they would be "packet-forwarded" to another Codec or Node if an alternative path exists on that route.



A combination of SureStream and Packet Forwarding, controlled by distributed intelligence

Packet forwarding means that no unnecessary audio decode and re-encode is required, a packet can simply traverse a codec or node en route to a final designated decoder.

Multicast / Multiple Unicast Relocation

Increasingly broadcasters are looking to IP networks to replace large broadcast audio distribution networks. Many of these networks have traditionally been provided by satellite distribution for either syndicated content delivery or for STL delivery where a large number of transmitters exist over a large geographical location. These satellite distribution networks are not without issues: it can be difficult and expensive to get permission to mount the necessary dish required for reception, especially in some metro areas where only part of the building is leased to house the radio station studios.

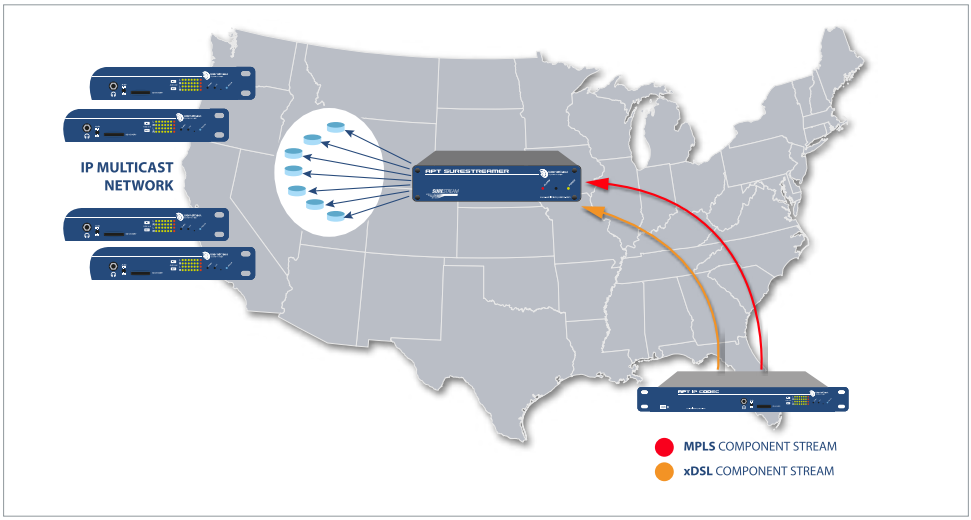
Reception of the signal is also a concern with ice and snow affecting the signal reception as well as rain fade. Hence, the interest in moving to IP.

For broadcasters deploying an IP codec network on a large scale where we are required to feed multiple decoders from a single encoder, relocating the multi-stream generation function of the IP audio codec away from the source encoder and closer to the decoders can offer significant benefit.
If Multicast is the preferred technology to be used in a large-scale network, it makes

financial sense to create a local Multicast node in the vicinity of several decoders that would offer significant cost savings over a national coast-to-coast Multicast cloud.

In the context of multiple unicast the benefits to moving the multiple unicast capabilities closer to the decoders are more concerned with reliability; the closer the generation of the multiple streams are to the decoders, the smaller the distance and number of hops these packets will need to traverse. Statistically this means that fewer packets are dropped, and, if Redundant Streaming is in use, this further reduces the chances of any duplicated packet loss on the component streams.

One way to create such a node is to use a product such as WorldCast's APT SureStreamer (see page 69). This box was designed initially to enable broadcasters using legacy IP codecs with a single port and no redundant streaming capability to bolt-on SureStream functionality to their existing infrastructure. However, as it does not need to be co-located with the sending IP codec, it can work well in establishing nodes such as those described above.



APT SureStreamer acting as Multicast or Multiple Unicast Node

NEXT… *in this section you should have developed a clear understanding of the methodologies used to overcome the challenges within IP networks. The next section aims to provides a deeper understanding of generic IP concepts. An understanding of these concepts can greatly assist in making choices about deployment and in the localization of faults and problem solving…*

6. Advanced IP Concepts

The previous chapters of this guide have sought to provide you with a solid background in the key elements that are involved in Audio over IP Networking.

However, there are some areas where a more detailed explanation of certain concepts or processes may be useful to you and help deepen understanding. This section of the guide outlines these in greater detail.

a The IP Layer & Protocols

The OSI Reference Model

The OSI reference model is used to easily explain the interaction between physical and logical connections in any communication system. It provides an abstract view of the techniques, protocols and services used.
According to the ISO/OSI reference model, communication in the network environment is based on seven layers with the full seven layer system being referred to as a stack. The lowest layers of this model represent network-oriented features and the upper layers are specific to each application.

In any communication system, the sender's interaction progresses from the top (layer 7) to the bottom (layer 1) and on the receiver side, in the reverse direction (layer 1 to layer 7).

For an even more simplified view the model can be reduced to a four layer model in accordance with RFC 1122. It loosely defines a four-layer model with the layers having names, not numbers. The image on the following page compares the two models, the ISO/OSI model and the "TCP/IP" Model.
The structure of the TCP/IP 4-layer model provides all we need for a better understanding of an AoIP application.

The Four Layers of the TCP/IP Model

The Link Layer (OSI layer 1 & 2)

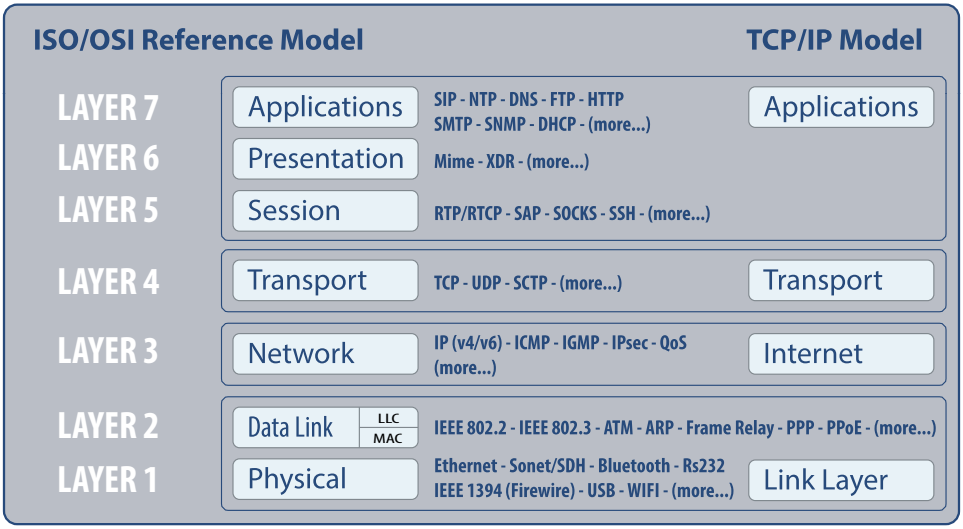
The basic function of the link layer is to provide the physical connection and continuous operational readiness. It is here that the electrical, mechanical, and functional parameters for physical transmission are defined. Other functions of layer 2 of the ISO/OSI model are assigned to the link layer:

The MAC protocol (Media Access Control)
Among other things, this protocol is responsible for managing the physical media access. It identifies connected hardware devices by their MAC address.

The LLC protocol
Logical Link Control is a sub-layer of the Link Layer in the TCP/IP reference model (ISO/OSI layer 2). It provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control mechanisms.

The Internet Layer

Using logical addressing, this layer selects a route for packet transmission from the source to the target device. This routing procedure selects a suitable path on the basis of different criteria, such as uniform load distribution, high data throughput, low cost or the highest possible security.



The Transport Layer

The Transport Layer provides a transmission channel for the communication needs of applications. The application does not need to know the particular characteristics of the transmission channel. UDP is the basic transport layer protocol providing a simple but unreliable datagram service. Therefore, the protocols of the higher layers must provide protection against false packet sequences or packet losses

The ApplicationLayer

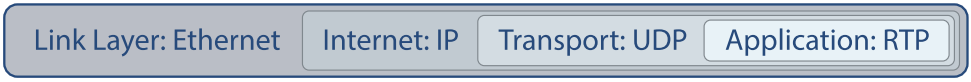
The application layer contains all the protocols that work together with the application's programs and use the network infrastructure for the exchange of application-specific data.

The application layer in the TCP/IP model is often compared as equivalent to a combination of the fifth (Session), sixth (Presentation), and the seventh (Application) layers of the full (OSI) model.

Encapsulation of Protocols and Services

In the OSI model, each layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path.

In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers, being further encapsulated at each level.



Encapsulation of protocol and services through the layer structure

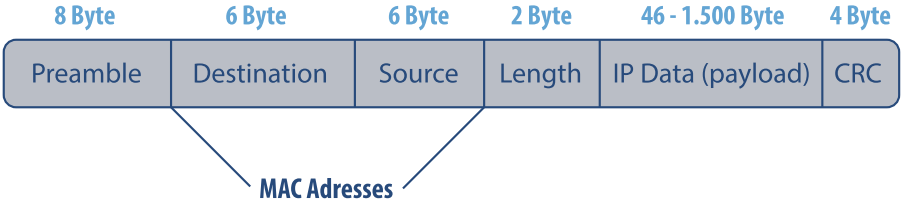
b MAC & IP Addresses

In order to exchange audio data or information between various participants in a network, it is necessary to have a method to accurately address and uniquely identify each participant. Within an IP Network, we use MAC (Media Access Control) addresses to identify each component. A MAC address is the physical address of an Ethernet component. It is unique worldwide and includes six bytes. The IEEE (Institute of Electrical and Electronics Engineers) manages the MAC addresses and assigns unique address blocks to the manufacturers of Ethernet components.
In the TCP/IP Model we have just studied, it is the link layer that manages the MAC addresses.

In addition to the unique MAC address that cannot be changed under normal circumstances, a network participant requires a logical address that uniquely identifies it on a network.

This is referred to as an IP address that can be assigned as a static address or dynamic address.

The relation between physical MAC and logical IP address is established via the Address Resolution Protocol (ARP). ARP is a protocol of the link layer.



Encapsulation of protocol and services through the layer structure

The image above shows an Ethernet frame; it contains the destination MAC and the source MAC addresses. The MAC addresses provide the relevant routing information.

IP addresses are on layer three - the ARP (Address Resolution Protocol) maps IP addresses to MAC addresses.

Internet Protocol (IP)

Internet Protocol Version 4 (IPv4) is the basis of today's IP networks. The next generation of this protocol (IPv6) is already currently in the implementation phase and will eventually replace the present one.
Version 6 is not only the basis of future IP networks but also that of third and fourth generation cellular mobile networks. It is the evolution of IPv4 and is therefore closely related and supports most of the features of IPv4.

In addition, however, it offers significant advantages as a result of major improvements. The IP address space has been significantly expanded and the package structure has been adapted to make the process much more efficient.
The Internet Protocol is assigned at the Internet layer (OSI layer 3). Routing is performed in this layer as is the coupling of subnets and network sections.

Packet Routing - General

The IP network has the task of delivering packets from the source host to the destination host based solely on the IP addresses contained in the packet headers. For this purpose, the IP network defines addressing methods that are used to label the packets with source and destination information.
The following sections describe how packet routing is performed in the IP network.

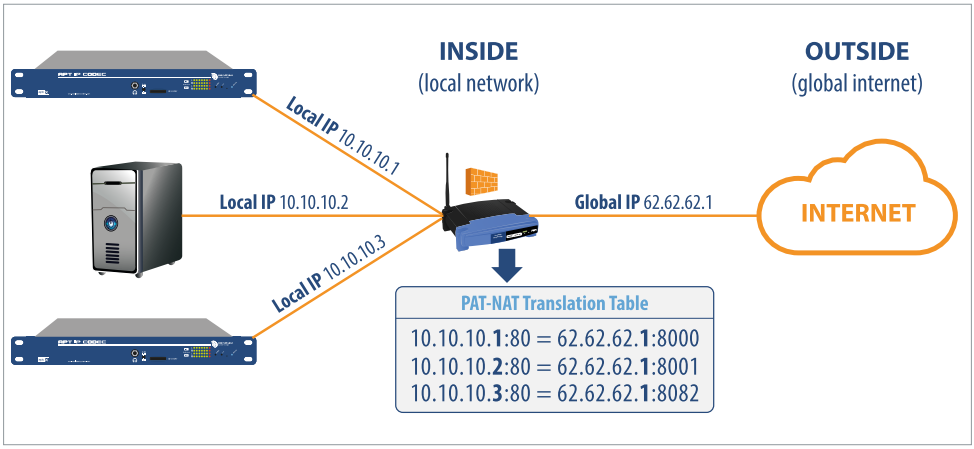
About Network Address Translation (NAT)

Network gateways are usually routers with additional functionalities. A very common feature of a gateway is the NAT feature. NAT is the collective term for procedures that automatically replace the IP address information in data packets with other addresses, to connect different networks. Therefore, they are typically used on routers and gateways.

Because of the limited availability of public IP addresses, NAT is mainly used to connect private networks with multiple IP addresses with only one public IP address to the Internet or wide area networks. This type of NAT is commonly known as "NAT overload".

The term "NAT overload" was initially established by Cisco and is derived from the fact that this method maps many private IP addresses to a single global address. In other words it "overloads" the real IP address utilizing port address translation or PAT.

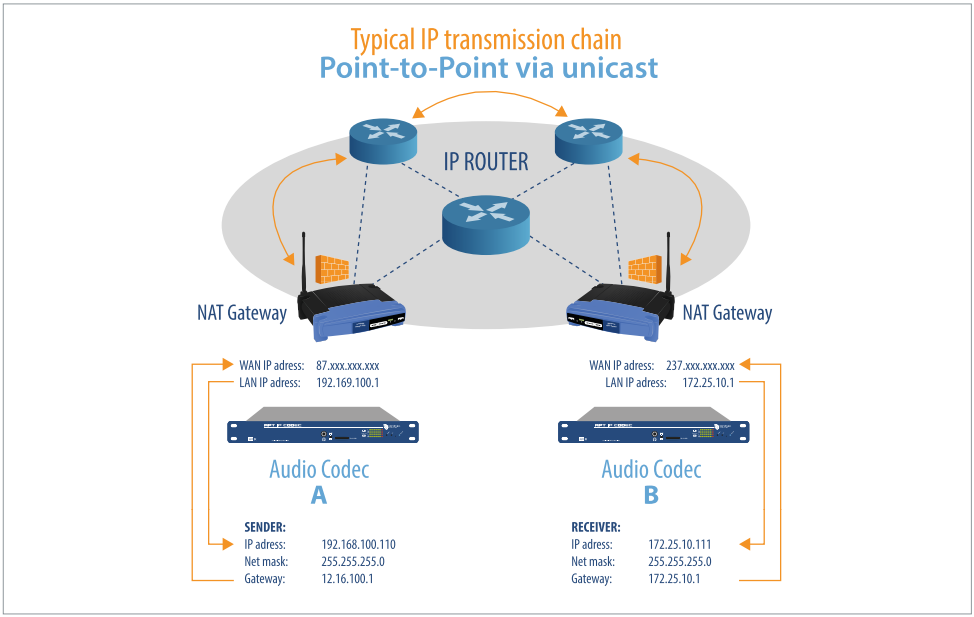
There are more types of NAT configurations in use, i.e. Pooled NAT or Static NAT. The image overleaf shows a typical NAT "overload" application: DSL lines are typically terminated by a NAT router connecting the local network to a public network. The NAT router acts as your gateway to which an audio codec must be connected.



The principal of NAT "overload" many-to-one IP address. The PAT/NAT table is stored in the router.

Routing and NAT

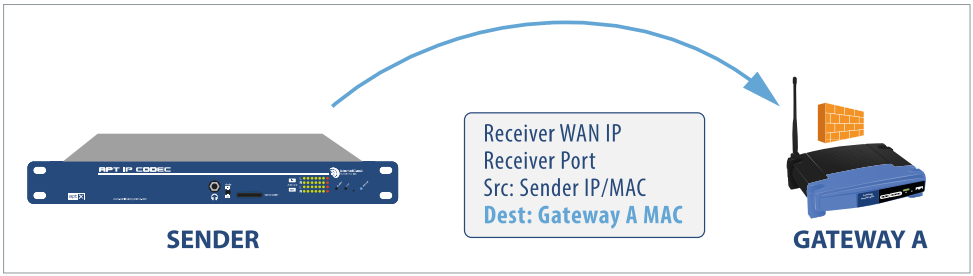
In general, packet routing is always required if the sender and the receiver are on different networks. If a codec sends audio data to a receiver which is outside his local network, the communication process works as follows (simplified):



The image above shows a typical point-to-point transmission chain

STEP 1

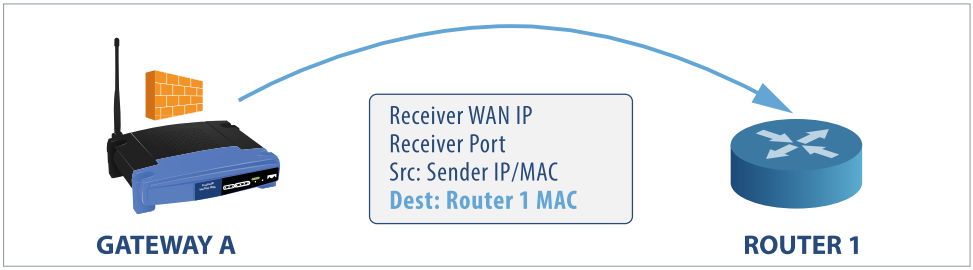
The sending codec (A) determines the nearest router (the gateway IP address); this is usually the local NAT gateway. Then the codec determines via ARP (Address Resolution Protocol) the unique MAC address (Media Access Control) of the gateway and builds the packets accordingly: The packets contain the destination MAC address of the local NAT gateway, the destination receiver's (B) WAN IP address (237.xxx.xxx.xxx), the destination port (e.g. 5004 for RTP payload) and the MAC and IP address of the sending Codec (IP 192.168.100.110). With this data in the header, the packet provides the necessary information to the IP network (source and destination). The local NAT gateway receives and processes these packets because they are sent to its MAC address.



The receiver WAN address is represented by the receiver's NAT Gateway (237.xxx.xxx.xxx)

STEP 2

Once the packets arrive at the local NAT gateway, it reads the destination's WAN IP address and, utilizing ARP, determines the next suitable router to which the packets should be forwarded. The packets are then modified to contain the MAC address of the next router, the destination receiver's WAN IP address (237.xxx.xxx.xxx), the destination port (5004), the MAC address and the public IP address of the source NAT gateway (87.xxx.xxx.xxx) as well as the payload, which remains the same. With NAT, the packets will go through significant changes at layer 3 (IP, OSI model) as they traverse the network.

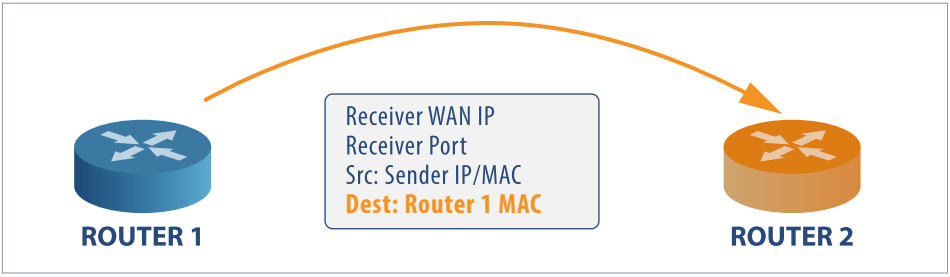


The NAT gateway replaces the source IP address with its own address on layer 3. A return stream will find the gateway as the destination IP address.

STEP 3

When processing in subsequent IP routers, the packets are changed only on Layer 2. The router determines the next router, identified by the MAC address utilizing ARP. The packets are rebuilt and now the destination MAC address is the MAC address of the next router and the source MAC address is replaced with its own.

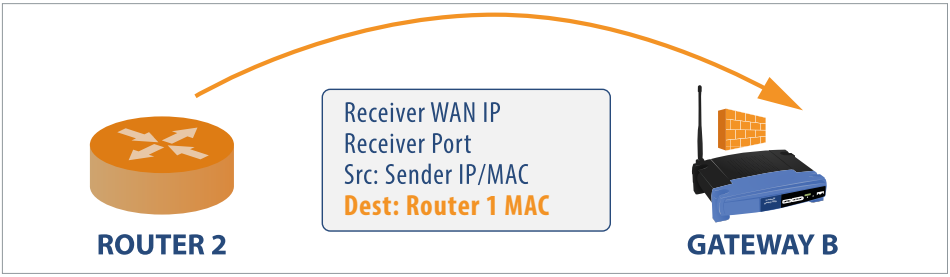
The WAN IP address of the final destination (receiver IP 237.xxx.xxx.xxx), the receiver port address (5004) and the source IP address of the NAT router (87.xxx.xxx.xxx) as well as the payload data are preserved. This means that on Layer 2 (IP), the packets are not changed again!



All subsequent routers in the network are changing source and destination MAC addresses on layer 2 only. The source IP address remains the sender's gateway WAN address.

STEP 4

This process is repeated until the last router finds the destination WAN address in the network; then the packets are as follows: they contain the MAC address of the last network router as source address, the MAC and IP address of the destination (237.xxx.xxx.xxx), the destination port address (5004), the IP address of the sender's NAT router (87.xxx.xxx.xxx) and of course the payload.

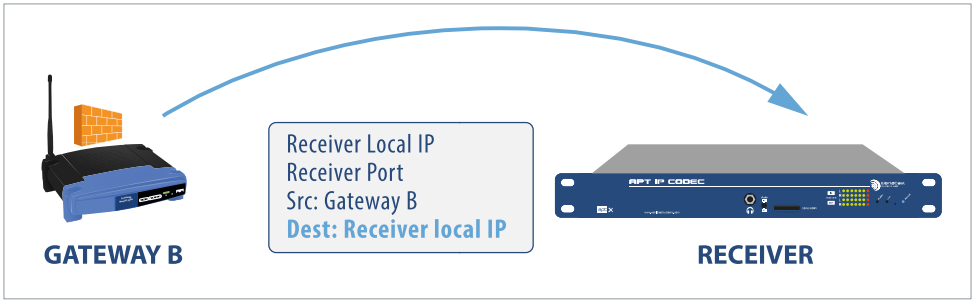


The receiver WAN IP address is represented by the receivers's NAT gateway (237.xxx.xxx.xxx)

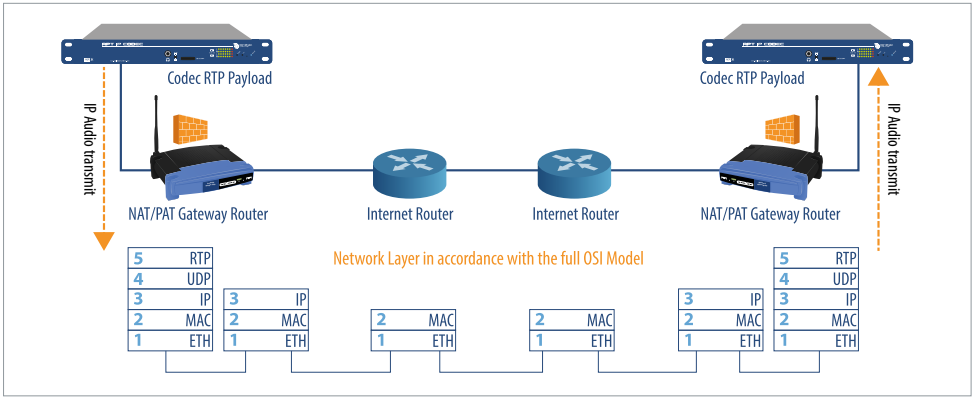
STEP 5

Finally the NAT/PAT table in the destination's NAT gateway maps the stream to the local IP address of the final destination (the audio receiver).

The image below shows the packet path through the network and layers of the (full) OSI reference model as described above.



The port information is used for mapping the stream to the final local IP address by the NAT gateway.



Internet routers do not change the layer 3 information again (Layer 2 router)

iv NAT Traversal Mode

The preceding paragraph explains the basic operation of routing and NAT. NAT "overload" allows the connection of a private network with multiple IP addresses on only one public IP address to the Internet utilizing PAT (Port Address Translation). Thus, multiple codecs and other services can be addressed through a single WAN address. NAT traversal techniques are typically required for point-to-point connections on the Internet involving codecs connected in private networks.

Codecs behind NAT-enabled routers do not have end-to-end connectivity on all services. One way to cope with this is to use a NAT traversal technique like STUN (Session Traversal Utilities for NAT). STUN is a client server protocol which provides information to the client on both the public IP address as well as information on the type of NAT behind which it is located. Utilizing STUN for NAT traversal requires a STUN server outside the private network domain. Another way to solve this problem is to use local port forwarding.

NAT Traversal via Port Forwarding

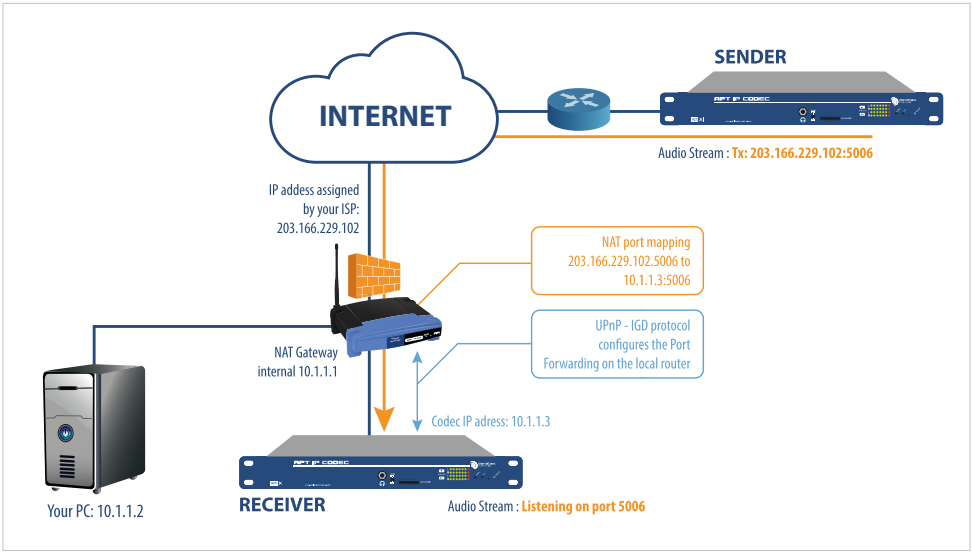
Unlike STUN, Port Forwarding doesn't require any external server or dedicated infrastructure. It is simply a matter of configuration, either manually or automatically on the local NAT gateway.

When configuring port forwarding, the network administrator assigns one port number on the gateway for the exclusive use of a service in the private network. For Audio over IP services, these settings can be complex and time consuming, as each individual audio stream requires a port forwarding configuration. Some codec brands such as APT have already implemented a method for configuring Port Forwarding automatically on the local NAT gateway via UPnP.

The Universal Plug and Play protocol (UPnP) provides a feature to automatically install instances of port forwarding in residential Internet gateways for individual audio streams. UPnP defines the Internet Gateway Device Protocol (IGD) which is a network service by which an Internet gateway advertises its presence on a private network.

A UPnP-supporting codec can therefore discover a NAT gateway and reserve a port number on the gateway, requiring the gateway to forward audio streams to its receiving port number and IP address (the socket for this stream).

The image below shows the principle:
In the diagram above the sender Codec sends IP audio to the global address of the NAT gateway on the receiver site on port 5006. The receiver is configured for receiving audio on its port 5006. UPnP IGD automatically configures port forwarding on the NAT gateway for this stream.



Port Forwarding utilizing UPnP IGD on the receiver site

v Static and Dynamic IP Addresses

An Internet Protocol Address (also known as IP address) is a numeric label assigned to each device (e.g. computer, audio codec) participating in a network that uses the Internet Protocol for communication. An IP address serves two principal functions: network interface identification and location addressing.
IP addresses are assigned to a network device (including codecs) either dynamically at the time of booting utilizing a suitable protocol, or permanently by fixed configuration of its hardware or software. A fixed configuration is known as a static IP address whereas, when the codec's IP address is assigned each time, this is known as a dynamic IP address. IP address assignment is related to the network structure to which the codec is connected. In some network structures, a static IP address may be advantageous while in other networks dynamic address allocation is required. A static address has the advantage that this codec is always reachable at this address.
The IP address of a receiver is the destination address which must be known by the sender, and if this address changes other techniques must take place to find the desired destination.

Today, on many networks DHCP (Dynamic Host Configuration Protocol) servers dynamically configure the IP address settings on network devices such as computers and codecs. A network is clearly structured in accordance with the logical organization of the radio station or broadcast company and may consist of different network segments linked by network routers. It is a common practice that these network segments are built of different subnets, each served by a DHCP server. A DHCP client is therefore essential on today's broadcast codec. If you are utilizing a standard xDSL link from any service provider in order to broadcast audio over the internet, the provider will allocate dynamic IP addresses via a DHCP server.

vi DNS and Dynamic DNS (DDNS)

Within an IP network, many different protocols and services work together to achieve a reliable service and one of the most important in public networks is the Domain Name System (DNS).

It is the directory of any hostname or domain name registered in the network. It translates easily understood or known names into the numerical IP addresses needed for the purpose of locating services and devices (including IP codecs) worldwide. As we have mentioned, DHCP servers and NAT gateways allocate IP addresses dynamically, so it would be useful if devices such as IP codecs could register their hostname with a Domain Name Service.

Today, numerous providers, called Dynamic DNS service providers, offer such technology and services on the Internet. DDNS is used to resolve a well-known domain or host name to an IP address that may change frequently.

It provides a constant addressing method for codec devices that may change their location or configuration by streaming to the registered hostname rather than to a dynamic IP address. Dynamic DNS is another technology which helps to automate the connectivity of a codec in a constantly changing network environment.

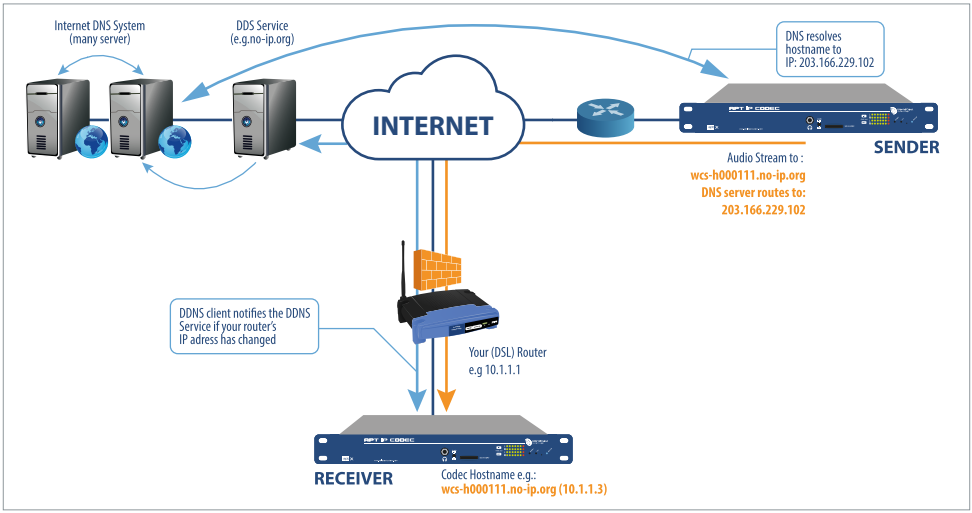
APT codecs from WorldCast Systems implement a versatile DDNS client which is capable of connecting to various DDNS service providers. The following diagram shows the interaction of the codec's DDNS client with the DNS system on the network.

APT codecs from WorldCast Systems implement a versatile DDNS client which is capable of connecting to various DDNS service providers. The following diagram shows the interaction of the codec's DDNS client with the DNS system on the network.

The sending codec sends the audio stream to the well-known hostname of the receiving codec (not the IP address). The DNS client in the sending codec makes a request that requires a host or domain name lookup and the internet DNS returns with the answer to the request. The example above asks for the IP address allocated to the hostname: wcs-h000111.no-IP.org, the answer is: 203.166.229.102.; this is the public address of a NAT gateway.

- The codec's hostname was registered by the Dynamic DNS service provider "No-IP.org".
- The name describes a device (the destination codec) registered at the domain "no-ip.org".
- The returned IP address information is the value from the internet DNS and describes the desired destination Codec.
- The destination codec hosts the DDNS client which permanently communicates with the configured DDNS service provider. Every minute the client reads the public IP address of the NAT gateway and sends this information to the DDNS service provider. Whenever the IP address of the NAT gateway changes, the DDNS service will update the internet DNS accordingly providing this information to all DNS requests.

Dynamic DNS is a technique that translates the static hostname to the dynamically changing IP address and allows the target codec to be located worldwide.



Principal of Dynamic DNS in the Internet

vii SIP and SDP

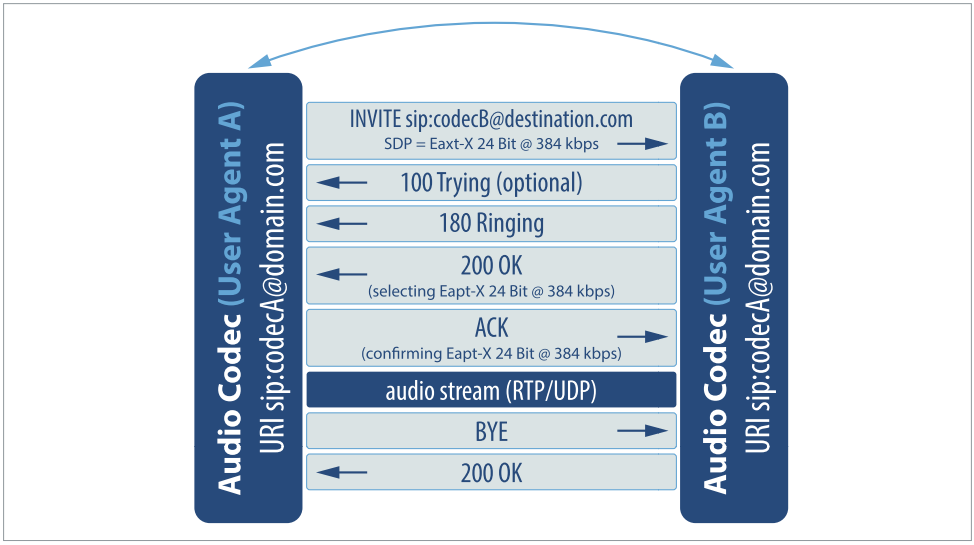
SIP is a signaling protocol and widely recommended by standards bodies. Until today typically IP Codecs were connected over private LAN or dedicated WAN but nowadays it is increasing common to connect codecs over any public network and using any service provider. Therefore a signaling protocol must be employed to make the connection. If this is not performed with SIP, Dynamic DNS and hostname streaming is still a suitable alternative.
SIP (Session Initiation Protocol) is a signaling protocol for creating, and terminating a session with one or more participants based on Internet Protocol (IP). A lightweight text-based protocol with only six messages, SIP minimizes complexity and is also transport-independent so it can be used with both UDP and TCP.

If there is TCP/IP and RTP/UDP available for the negotiation, RTP over UDP is mostly used for the media data transport. As a peer-to-peer protocol it is possible for individual components to connect directly without any central server unit. An individual component in the context of SIP is called a user agent and has its own SIP URI (Uniform Resource Identifier).

The syntax of a SIP URI is similar to an email address sip:user@host. "User" is a pre-defined user name, while the host is a domain name or network address, e.g. sip:myCodec@myDomain.com. In a situation where one user agent (A) wants to connect another user agent (B) without a connecting device in the middle, user A must know the SIP URI of user B (see figure below). If user B changes his location into another network, then the temporary SIP URI changes as well.

In larger or globally connecting systems a SIP proxy server will be required to forward and connect SIP calls towards the intended destination. Once a codec has registered to the SIP registrar server, the codec's current (temporary) SIP URI will be forwarded to the SIP location server. The location server makes the current SIP URI of this codec available to the SIP proxy server that is negotiatingthe connection.

SIP/SDP communication peer-to-peer



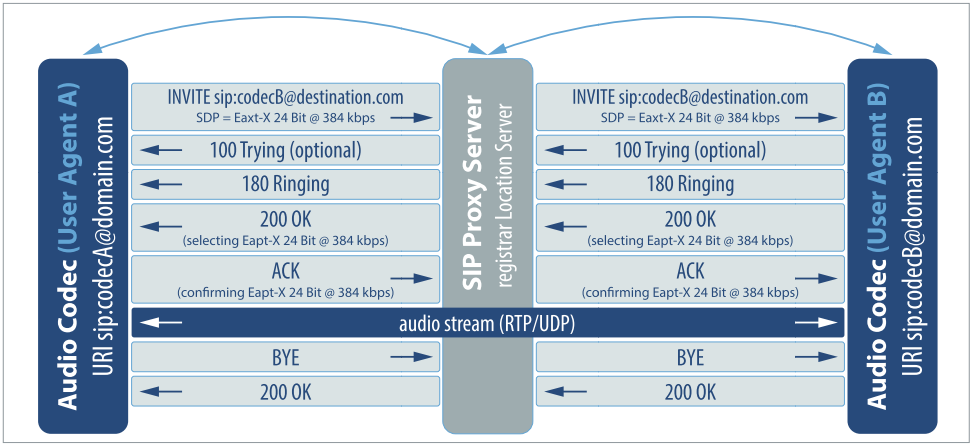
Peer-to-Peer connection without SIP proxy and location server

With this mechanism, the codec is visible globally and a SIP call can be established regardless of the codec's current location. The location server is a big database; it translates between temporary SIP URIs and home SIP URIs.

SIP acts as a carrier for the embedded Session Description Protocol (SDP). SDP has the role of negotiating the properties of a media data connection. It describes the media content of a session, e.g. what IP port to use, the algorithm being used or exchanging priority lists, which can be replaced or modified by the remote site. Once the connections have been made, SIP endpoints simply exchange media streams – typically using RTP over UDP.

SIP can be understood within the context of ISDN connections and media transport mechanism in the IP domain. The ISDN D-channel is responsible for negotiating a connection and the media data are carried

SIP/SDP communication through SIP infrastrucutre



Simplified SIP/SDP communication on SIP infrastructure for Codec A and B

on the ISDN B-channels. SIP does the session negotiation and manages the connections; the RTP/UDP or TCP/IP transport mechanism represents the media transport in an IP network. With SIP the process of connecting and media transport can be on different networks.

viii STUN (Session Traversal Utilities for NAT)

STUN is a standardized set of methods and a network protocol that allows an end host (the Codec) to discover its public IP address if it is located behind a NAT router (refer also to NAT traversal mode). The STUN protocol allows SIP operating behind a network address translator (NAT) to discover the presence of the NAT and to obtain the mapped (public) IP address and port number that the NAT has allocated for the Codec's UDP stream.

STUN requires a STUN server located on the opposing (public) side of the NAT, usually the public Internet.

The codec device behind a NAT router runs the STUN client; the STUN client communicates with the STUN server via STUN binding requests and STUN binding responses. The response of the STUN client allows the SIP user agent (in the codec) to use the public contact information for the SIP header or to modify the SDP parameter.

IX VLAN Tagging

A computer network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN.

In the context of IP Codecs, VLANs are beneficial for logically separating the management network from the audio streaming domain. Nowadays the majority of IP audio codecs provide two ethernet ports for multi-purpose use.

Usually the software allows configuration of one port as a streaming port and one port as a management port. This is a suitable approach as long as a single port for audio streaming is in use. But if both ports must be used for redundant streaming the management must share one of the physical ports.

This is possible if the codec is VLAN enabled and the codec can generate VLAN tags.

VLAN tagging as described here, is a protocol based method and defined in IEEE 802.1q. As indicated, a VLAN router is able to accept tagged packets from different VLANs while keeping these packets strictly separate. VLAN switches are physically connected to other VLANs via the so called VLTs (VLAN trunk Ports).

The data capacity between the switches are limited by the network design, nevertheless, the IEEE 802.1 protocol set allows a packet periodization for each assigned VLAN on these trunk ports. This is described in IEEE 802.1p

A codec that can mark packets through tagging offers great benefit. It can physically connect to each VLAN enabled switch or router that is connected to the other VLANs via the trunk port. This means it is not necessary to install a new physical infrastructure from the codec location to the next assigned VLAN device.

A codec should be able to manage a number of virtual interfaces for audio streaming and management services in accordance with IEEE 802.1q & 802.1p.

NEXT…*with a better understanding of how IP Networks work, there are many test tools that can help you on pre deployment of your AOIP network and also on solving problems, the next section outlines just a few …*

7. Network Testing & Analysis

Pre-Deployment

Before you ever receive your audio codecs there are many tools that can be utilized to see just how a network can perform. I use the present tense "can" and not the future tense "will" in the previous statement as IP networks, if we are talking about the open Internet, can have hugely variable performance form one day to the next day and from one hour to the next hour. This variance in delay is due largely to the contended nature of the bandwidth we use to connect to the open Internet.

Typically xDSL connections are contended or shared with other users at ratios of 1:25 i.e. one piece of bandwidth shared between 25 potential users. At 8 P.M. in a residential area then we can see a spike in usage as people switch on their Netflix service or other media streaming services, the contention ratio is much higher than say at 12 A.M. in this type of area and on this type of link.

So pre-deployment testing can give you an idea as to whether you can go it alone on a single link or whether you may need to look at a redundant streaming technology, such as SureStream to enable the open Internet to deliver an acceptable service for your STL and another broadcast audio links.

In the context of managed IP links such as MPLS, WAN, LAN the same tools are used but the context will be different though. In this scenario you will be measuring a very high level of performance (you hope) and seeing whether the MPLS link is in line with the Telco SLA or whether the piece of bandwidth that the IT guys promised to carve out of the corporate LAN with a guaranteed bandwidth and QOS is up to spec.

This section looks at the basic tools required pre and post deployment and explains the application of these tools in preparation for an IP codec deployment.

Ping Test

This is the most basic network test of connectivity between the two end points you hope to connect with your audio codecs. The ping test has the syntax as illustrated on the next page and is usually originated on a PC or network device at the sending site to another PC or network device at the receive site.

For Windows users, the basic command in a command window (CMD) is ping xxx.xxx.xxx.xxx where the Xs represent the IP address of the target. Pings can also be sent to a URL, provided that a valid DNS server setting is configured on the originating PC. Adding -t to the syntax after the IP address will allow you to run a continuous ping and can be useful if you are trying to physically find the correct RJ45 to patch to the send or receive PC.

Ping is only an indication of the fact that the two ends are available and visible. However, the ports on which the audio codecs need to connect and be managed will also need to be open and available. A ping operation cannot determine this.

Ping is a good indication of round trip delay between the two end points and also the levels of jitter on the network.. What ping is not, however, is an indication of packet drop. This point is sometimes misunderstood. If someone runs a ping -t for a few days and sees no dropped packets they mistakenly believe their link is clean and ideally suited for IP audio codecs.

This assumption is incorrect as ping uses minimal bandwidth and the ICMP protocol so any dropped packets will be present if the receiver does not send an acknowledgement (ack.) packet to the sender.

Audio codecs for a variety of reasons, not least latency, use UDP-IP (connectionless or send and forget) so a ping has no relevance to packet loss as the protocols are different. There is a different tool for this purpose.

```
C:\Users\kcampbell>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break:
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Head
er).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Ping syntax viewed through Command prompt in Windows

```
C:\Users\kcampbell>ping 66.166.242.173

Pinging 66.166.242.173 with 32 bytes of data:
Reply from 66.166.242.173: bytes=32 time=192ms TTL=240
Reply from 66.166.242.173: bytes=32 time=209ms TTL=240
Reply from 66.166.242.173: bytes=32 time=233ms TTL=240
Reply from 66.166.242.173: bytes=32 time=151ms TTL=240

Ping statistics for 66.166.242.173:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 151ms, Maximum = 233ms, Average = 196ms
```

Ping from Belfast to codec located in Miami, giving average round-trip delay

In summary then Ping can help establish whether the equipment is live and reachable and also what the level of jitter is on the network. The jitter figure can be calculated by subtracting the lowest variable from the highest, the resultant millisecond figure can then be manually inserted together with some overhead, to allow for a variation over time, into the jitter buffer setting on the audio codec.

IP Connection Verifier (UDP Test Tool)

The IP Connection verifier software tool has been specifically developed by APT and can be provided free of charge to any customer or prospective customer. It is essentially a simple UDP packet generator and receiver that runs on any PC.

The idea is to generate a stream of UDP packets and simply count the number of received packets at the far end of the link. This will give you a crude percentage loss of packets on the link you intend to use for your IP Codec deployment over a period of hours and days. It can be thought of as a UDP Ping tool with logging!

There are several tools to enable the testing of a link's throughput or bandwidth. What you can measure on an open Internet link and a managed link is different but the tools are the same.

On a managed link such as MPLS the bandwidth, just like the packet delivery, should be constant and unchanging within a predefined range. The bandwidth on an MPLS service from a Telco should be stated in a SLA or line rental agreement and should not significantly deviate.

Therefore if you have a service that guarantees a bandwidth at 1.5MBits per second then you should always be able to measure the bandwidth and achieve this figure.

However because of the contended nature or sharing of the connectivity with other users on the open internet, bandwidth, just like dropped packets is affected by the number of subscribers or users fighting for that bandwidth. So on the open Internet a bandwidth up-link (egress from the site) and down-link (ingress to the site) will be highly variable depending on the subscribers competing for the bandwidth through the various hops from point A to point B at that particular time.

Illustration of UDP Test Tool Bandwidth on the link

Added to this is the fact that if you use a software tool like those listed below to measure the bandwidth on an open Internet link you only measure the egress and ingress to that point, this will not in fact measure the bottlenecks to bandwidth which can be further downstream.

http://www.speedtest.net/
http://www.bandwidthplace.com/

Trace Route or Hop Analysis

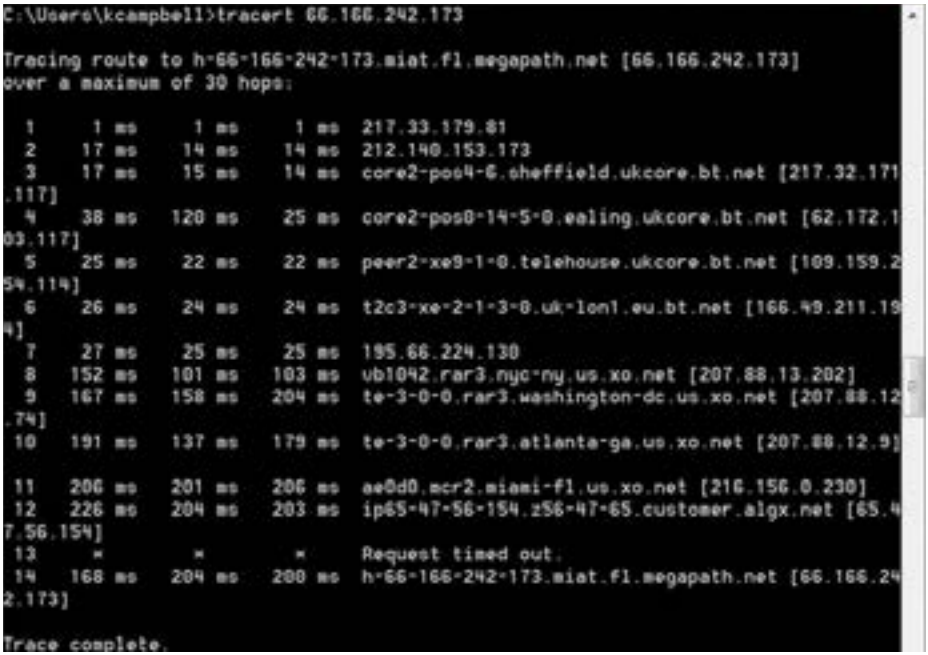
A hop is simply an intermediary device along the path between your two codecs. This can be a router or a gateway between networks. The number of hops will have an effect on latency, the likelihood of dropped packets and can also have an effect on the available bandwidth. Its logical to assume that more hops equals more latency and more chances of encountering a bandwidth bottleneck. So where possible keep the number of hops to a minimum. Easier said than done!

Unless you have an MPLS or a managed circuit, once you leave your facility you're at the mercy of the open Internet and the packets will dynamically traverse the Internet as best they can. The trace route (CMD window syntax tracert xxx.xxx.xxx.xxx) you perform now may differ significantly from the one you did five minutes ago.

There are some Internet providers which claim they can keep you "on net" for as long as possible, limiting the number of hops for at least a portion of the open Internet journey. However eventually the packets will have to pass through a Gateway onto the real Internet and at that time obviously control is lost.

Bandwidth Requirements

Now that you have confirmed the veracity of the link using the IP Connection Verifier or possibly confirmed that a single link is not sufficient and have opted to use a redundant streaming approach, you still need to calculate the bandwidth required on each link. As we learned in the previous chapters, the bandwidth requirement is composed of the audio payload plus the packet header information.



Traceroute from Belfast to Miami

Larger Packet Size = Less Bandwidth Requirements = Greater latency
Smaller Packet Size = More Bandwidth Requirement = Less latency

If we use the example of the audio algorithm, Enhanced apt-X, 16 Bit at a data rate of 256 kBits, a defacto standard for lossless STLs at 15kHz FM quality, the data requirement Packet

Size = 512 Bytes

Audio Rate bits/sec	Pkt/Sec	Overhead Bytes/Sec	Tot Bytes/ Sec	Bits/Sec Absolute	kBytes/ Sec	kbits/Sec	Packetisation Delay (mS)
256000	62.50	3375.00	35375.00	283000	34.55	283.00	16.00

Packet Size = 64 Bytes

Audio Rate bits/sec	Pkt/Sec	Overhead Bytes/Sec	Tot Bytes/ Sec	Bits/Sec Absolute	kBytes/ Sec	kbits/Sec	Packetisation Delay (mS)
256000	500.00	27000.00	59000.00	472000	57.62	472.00	2.00

varies significantly: So, by using a 512 Byte packet size rather than a 64 Byte packet size the data requirement on the link has reduced significantly from 472 kBits to 283 kBits. The delay however has increased from 2 to 16 msec. This delay figures relates only to the packetization process and must be added to the hardware and software codec propagation delay and the network delay to have a true end-to-end or round trip delay.

In summary, then the packet size selected will have a big effect on the bandwidth required on each link, the trade-off here is always between tolerable delay and bandwidth usage. We don't expect you to do this math for each situation, APT have a number of free issue spreadsheets and calculators which can calculate bandwidth usage for any algorithm based on any packet size selected.

These calculators relate only to the APT hardware range and implementations, they can however be used as a guide to other OEM requirements.

Troubleshooting

Occasionally things will go wrong and in that respect IP Audio is no different than the previous audio transport technologies that have preceded it. Where IP Audio has the clear advantage however is the range of backup and redundant options that can be implemented and at a non-linear cost. The market leading example of one of these technologies is our very own SureStream technology.

If you have planned and implemented your IP Audio network correctly, the off air outage due to an STL failure should be a thing of the past. Consequently, troubleshooting the IP Audio STL or contribution link can be less stressful than the STL or audio transport issues of the past.

However, the complexity can be overwhelming and interaction with several third parties from the audio codec vendor to the link provider to the IT Department can be required to localize and fix an issue.

The same tools that you have used in pre-deployment testing can also be used in the troubleshooting process, so PING is used to establish that the far end codec is alive and visible on the network.

IP Connection verifier can confirm that the percentage packet drop is broadly within range of the benchmarks recorded when you have done the pre-deployment testing with that same tool.

Trace Route can confirm again that the number of hops is broadly within the pre-deployment benchmarks that you have recorded. The importance of benchmarking and record keeping with regards to network

Example of network tools, Logging on the Speedtest.com IOS App from Ookla and a LAN Scan from the IOS App of Net Analyser by Technet.net

performance can't be over emphasized. As mentioned earlier the network performance especially over open internet is completely variable so to have a "mean" performance of each link or network is absolutely useful when troubleshooting.
As well as these very basic tools to help troubleshoot and localize problems, there are many more that can enable more detailed analysis. Typically the "average" broadcast engineer will pass network related issues to his IT staff or service provider, once it is determined that the issue is with the network itself. Increasingly however we are also seeing CISCO and Juniper certified professionals being part of the broadcast engineering team! This is a trend that will continue for sure.

Troubleshooting & Emulation

Some IP Audio codec providers also assist customers with fault diagnosis and analysis of networks as part of an on-going commitment to customer care. WorldCast Systems is one such organization. Some of the tools we use to great effect include network capture and emulation. We have a very comprehensive test bench in our main R&D site in Belfast. One specific tool is our troubleshooting arsenal is the WAN Emulator range from Apposite Technologies.

WAN Emulators allow the simulation on the bench of all the typical characteristics of IP links including bandwidth, jitter, latency, packet drop, LOCs etc.

These emulators are vital tools in developing robust products to meet the real world demands of the huge array of IP networks and conditions encountered.

With regards to troubleshooting, WorldCast Systems can issue a recording tool to any customer globally. This recording tool can be deployed on a single PC or laptop and is used to capture exactly the performance on a specific network from point A to point B. This capture can then be emailed to our R&D Department where it is loaded to the emulator and then we have your network sitting on our test bench with a full set of test tools and a team of engineers and developers ready to analyze any problem specific to your network.

By using emulation through your IP codec provider as a tertiary troubleshooting tool, some very specific underlying network issues can be discovered very quickly.

In the past emulation has helped us find issues for our customer base related to deficient router buffering and queuing to packet threshold settings on the providers IP backbone. Once diagnosed through emulation the fix is more often than not a network change or on occasion a codec firmware change and subsequent release.

Emulator Monitoring Interface

NEXT…*now you have the "knowledge" it's time to do a final Audio Over IP Pre-Deployment checklist, the next section has exactly that…*

8. Pre-Deployment Planning

In previous editions of this booklet, we have published a Checklist with our recommendations for a broadcaster about to embark on their first Audio over IP Deployment.

As time moves on and technology advances, this type of checklist becomes less useful. With a multitude of options to choose from, there is no longer a "recommended strategy" to fit all users; you can tailor your IP audio network to meet your station's own particular requirements.

Therefore, our closing advice is no longer a series of Do's and Don't's but a more a list of Points for Consideration to ensure that all the relevant points are well understood before committing to any purchase or contract. With the information learnt from this guide, you will be in the best position to decide what is right for your installation.

1 Network Selection

With an understanding of the different types of IP links that can be made available, you can knowledgeably research the market to investigate the options available to you from your local service providers.

Your ultimate choice will be affected by the following considerations:

- The type of broadcast link required. Is this a permanent STL or distribution link or a temporary remote connection?
- The distance of the connection. A local hop is likely to involve a single service provider and offer higher quality and reliability of connection. Should you need to link up national or international sites, this will have a significant impact on the reliability and delay that is to be expected. Be sure to establish if multiple carriers are involved.
- Availability of connections. Different Service Providers will offer different solutions and you may not be able to access all types of connection from each. For managed links, a detailed study of the Service Level Agreements (SLAs) offered should provide you with a deeper understanding of the level of reliability to be expected.

2 Data Plan / Service Selection

- Your data requirements. You will need to calculate in advance the bandwidth you would need for all links based on the type of content, connection (unicast, multicast or multiple unicast) number of audio channels and coding algorithms used.
- Your business requirements. Some stations may choose not to operate a dedicated link for audio connections but instead share a large corporate connection (often fiber or managed IP) with their daily business operations. If this approach is taken, it will be necessary to implement QoS throughout the internal network to ensure that the audio is given priority.
- Your budget. It must be mentioned that quite often the perfect solution for audio transport may be outside your budget constraints. In this case, compromises may be required.

3 Equipment Selection

A typical IP network is made up of much more than just links for audio transfer. A professional approach to audio transport over IP requires mastery of not just the network, but also the suite of hardware and software tools which allow control, supervision and operation of packetized audio delivery.

These tools enable not only network and equipment monitoring, but the implementation of remedial action, hardware redundancy and fault alleviation. Where possible, the broadcaster should seek to source an integrated solution which delivers all these services in a single product, specifically the audio codec.

This integrated solution allows the administrator to manage both audio AND data services from a central location either by a unified control software or on a higher level by SNMP. Among the factors to be considered when comparing equipment are:

(a) Design Philosophy

The design philosophy behind products is a key factor to consider when purchasing equipment for use in a professional broadcast environment. There are two key approaches: DSP-based or PC-based product development.

PC architecture uses off-the-shelf motherboards which are generic, low cost platforms not designed for use with audio or 24/7 operation. Instability and memory leaks within the operating core can lead the system to "hang" as a PC is prone to do.
DSP-based systems on the other hand are designed from the outset for high quality audio delivery and signal integrity. They typically offer faster boot-up operation, much greater stability and a significantly greater operating bit depth (resolution).
While it may be acceptable for a home user to reset their PC, it is definitely not acceptable for professional broadcast applications and PC-based architecture should be avoided for "always on" processor intensive applications.

(b) Redundancy

For mission-critical STL applications, hardware redundancy is vital to ensure back-up in the case of network or equipment failure. A broadcaster must consider the importance of each link and source equipment that conveniently provides the necessary fail-safe options. Hot-swappable audio modules, redundant power supplies and automatic backup functionality are just some of the options that should be considered.

To ensure even greater reliability, a codec should support Redundant Streaming technology such as APT's SureStream which provides "Always-On Redundancy".

SureStream works in such a way that there is no "main" and "back-up" link but each connection contributes to the stream. This means there is no glitching or delay when switching to a back-up rather that the service remains seamless no matter what is happening on any of the contributory links.

(c) Configurability & Quality of Service

As noted throughout this booklet, there are many variables in the world of IP networking. It is therefore vital that the audio codec selected provides the broadcaster with the flexibility and control to manage anomalies on their IP network and get the best quality audio performance from the bandwidth available.

This will typically include audio setting configuration, control of packet size, ability to buffer audio to compensate for jitter, and the ability to set Quality of Service at the transmission point. The codec should also provide maximum flexibility with

regards to network configuration, allowing the broadcaster to easily implement unicast, multiple unicast and multicast applications.

(d) Audio Algorithms

Having prepared your IP network for audio transport, the next step is to choose the best method of sending audio down the link. Restrictions in available bandwidth may rule out linear/PCM audio and some form of compression is usually required. There are two main types of compression techniques: ADPCM and Perceptual algorithms.

Perceptual based algorithms (such as MPEG L2, MPEG L3 (MP3), AAC and their many derivatives) use psycho-acoustic based principles which analyze audio content and determine what is audible to the human ear. The algorithm will remove all inaudible content and is therefore, by definition, "lossy". Using multiple passes of a perceptual codec (for example, consider the broadcast chain for HD Radio or DAB) will result in content heavy with artifacts. Ultimately this will cause "listener fatigue," swiftly followed by tune-out to a station offering higher audio quality.

Additionally, perceptual coding will introduce a delay to the audio delivery which is generally unacceptable for real-time audio applications. Working on the assumption that the IP transport stream and packetization will naturally introduce a minimum delay of 20 milliseconds, it is imperative to minimize the latency of the compression algorithm employed. In essence, using a perceptual coder, even a low delay variant, will render the solution unusable for any level of real-time broadcast such as talkback applications and off-air monitoring.

ADPCM algorithms offer a more attractive alternative given their gentler, non-destructive approach to coding. ADPCM-based, Enhanced apt-X® technology delivers both exceptional acoustics and ultra low delay, making it particularly suited for audio over IP applications. Enhanced apt-X® overcomes the problems associated with multiple psycho-acoustic passes of audio in the broadcast chain as it is extremely resilient to tandem coding, retaining acoustic integrity up to and beyond 10 encode-decode cycles. Along with the well-documented features of low latency and audio performance, Enhanced apt-X® also features AutoSync™, an embedded word pattern which aids connection and synchronization and complements the packetizing nature of UDP/IP.

As a non-frame based algorithm, Enhanced apt-X® allows for smaller packets (as small as 64 bytes) contributing less delay and enabling quicker synchronization. The ability to start synchronisation on receipt of the next valid sample and to achieve full synchronisation within 3ms @ Fs=48kHz ensures faster recovery from packet loss, making dropouts less audible.

(e) Management & Monitoring

With a wide number of variables and constantly changing network conditions within the field of IP audio networking, it is vital that broadcasters have access to extensive control and monitoring capabilities. This can be achieved either by front panel control, SNMP or a dedicated Management System software package.

Whichever option is selected, the user should ensure that it provides them with the following capabilities:

- At-a-glance status of all codecs throughout network
- Flexible configuration of audio settings: algorithm, sample rate, data rate, mode etc…
- Ability to define audio profiles for quick and simple configuration
- Flexible configuration of transport link. For IP, this will involve setting up packet size, jitter buffers and IP unicast and multicast routes, back-up links
- Performance Monitoring providing statistics on packets transmitted and received, error counts, sequence errors etc...
- Ability to set critical, major and minor alarm conditions relating to issues such as silence detection, loss of connection, loss of sync & exceeding jitter buffers
- Ability to set conditions which are triggered on alarms i.e. switch to automatic backup and revert after nsecs of stable audio stream.
- Alarm and Event Logs to enable analysis of recurring errors and conduct accurate network diagnostics.
- Remote Software Update Controls

(f) Distributed Intelligence

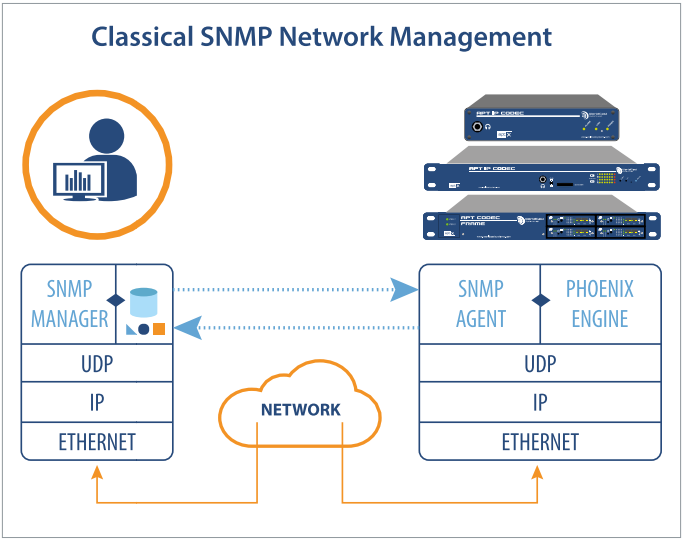
On top of the basic monitoring requirements listed above, APT codecs offer a sophisticated solution that builds an even greater degree of intelligence into your network. Based on ScriptEasy, the intelligent scripting application from our partner company, Audemat, APT codecs allow you to tailor the behaviour of both your codec and co-located equipment so that not only are you alerted of any issues or concerns but that, should a trigger event occur, the system can automatically take the action you require to remedy the situation. In many cases, your back-up plan can be in place and running before you are even aware that there has been a fault! ScriptEasy can also provide consolidated monitoring by aggregating data received via SNMP with controls from traditional I/O and summary data into a user-friendly dashboard view.

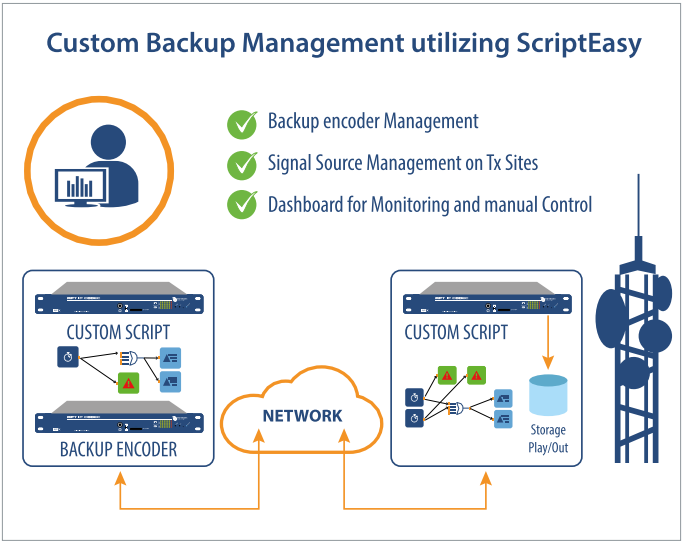
Status Screen on the APT IP Codec Interface shows audio configuration and current connection status.

This dashboard will provide simple graphical statuses of many different parameters across several units in your network.

Amongst many other things, ScriptEasy enables you to:

- Create & manage many individual back-up scenarios
- Use the GPI/GPO system to reconfigure the local and/or remote unit on the fly
- Get confirmation of actions triggered by SNMP or GPI/GPO
- Define your desired logic sequence of alarm conditions that will trigger an action or create an alert
- Setup a complete SNMP communication system
- Visualize the current status of many remote-located devices





9. APT's IP Codec Solutions

APT IP Silver

The APT IP Encoder Silver and IP Decoder Silver combine to enable affordable yet professional delivery of audio content over IP networks.

Low on cost but rich in features, these units are perfect not only for standard broadcast applications such as STLs and confidence monitoring, but also for commercial IP audio distribution in retail, hospitality, hospitals, campuses and many other applications.

- Low cost separate Encoder & Decoder
- Professional XLR connections
- Compact ½ x 1U unit
- Standard algorithms include professional Enhanced apt-X & linear audio, MPEG 2/4 HE-AAC v1/2 coding
- Features APT's SureStream technology for seamless, broadcast-grade audio over public IP links - see page 69 for more details
- Intuitive web-based browser control
- Intelligent Control with ScriptEasy

APT IP Codec

Perfect for STLs and mission-critical applications, the APT IP Codec offers the most complete set of IP features ever included in APT's extensive range and features both our revolutionary "SureStream" technology and intelligent ScriptEasy scripting.

- Professional duplex stereo IP audio codec
- Support for Unicast, Multiple Unicast & Multicast
- Dual IP ports configurable for back up
- DSP-based architecture for 24/7/365 reliability
- Redundant Power Supplies
- Wide range of algorithms: Enhanced apt-X algorithm & Linear PCM, MPEG 1/2 Layer II, MPEG 4 AAC LC/LD/ELD & MPEG 2/4 HE-AAC v1/2
- Highly Intuitive Network Management Software (NMS)
- Embedded Web Server for control from any location
- Embedded Auxiliary data for transmission of RBDS / RDS or PAD
- Up to 4 Opto-coupled Inputs and up to 4 Relay Outputs
- Support for SNMP, Alarm & Event Logging
- Intelligent Control with ScriptEasy
- SureStream for broadcast-grade reliability and audio quality over open internet links

APT AoIP Multi-Channel Frame

SURESTREAM

The APT Multi-Channel Codec (formerly known as the WorldNet Oslo) is a favored platform among Radio Broadcasters for the transport of multiple channels of audio, data and voice across IP or E1/T1 Networks. With a modular, single-platform approach, multiple layers of redundancy and exceptional scalability and flexibility, it is the perfect solution for STL, TSL, Remote broadcast, backhaul and studio linking applications.

The APT Multi-Channel AoIP Codec can support up to 16 channels of audio within a single unit of rackspace - and even more IP streams when using multicast or multiple unicast technology. The 1U APT Frame will accommodate up to 4 AoIP modules, each equivalent to a stand-alone stereo duplex codec combining audio, dual IP transport and auxiliary data on board. Up to 8 AoIP modules can be accomdated on the 3U Frame.

- Flexible & scalable system
- Transports up to 2 stereo audio channels per module
- Deliver up to 24 IP audio streams per module
- Four Independent Clock Domains per module
- Low delay, Enhanced apt-X or pure Linear audio plus other coding options
- DSP-based for 24/7/365 operation
- Redundant Power Supplies
- Hot-swappable modules
- Embedded WEB GUI can be accessed from a web browser or the NMS
- Auxiliary Data and GPI/GPO
- Offers full range of audio formats: simplex, duplex, AES/EBU, AES/EBU with analog backup, analog with HI/LO or 600Ω impedance.
- Point-to-Point and Point-to-Multipoint operation
- Supports a variety of protocols including: UDP RTP/RTCP, SIP/STUN#, SAP#, DHCP, DDNS, NTP, IGMP, ICMP, VLAN Tagging#, SNMP, UPnP
- Award-winning SureStream technology

APT SureStreamer

For broadcasters who wish to benefit from the cost savings and reliability offered by SureStream but don't want to invest in new Codec hardware, the APT SureStreamer is the perfect solution. It sits in front of existing single port IP Audio Codecs enabling the use of easily affordable IP connections to deliver broadcast-grade audio with no interruptions, glitches or drop-outs. It continues to provide a seamless audio stream, even when one of the contributory links suffers a total Loss of Connection. Using either two separate wired internet connections or one wired, one wireless (i.e. DSL plus 3G/4G), the APT SureStreamer ensures that one perfectly seamless, reconstructed stream is received with the reliability & audio quality you expect from an E1/T1 using easily affordable public internet connections.

SureStream Summarized

Throughout this booklet, we have noted that there are many benefits to be gained by migrating to IP networks but that these also present many challenges for audio broadcasters. You cannot simply rip out your T1 and replace it with a DSL tomorrow. So we need to find a clever way of exploiting the cost advantages of IP without suffering the disadvantages.

APT's SureStream technology is an innovative and multi-award winning approach that is currently enabling broadcasters throughout the globe to transport their broadcast audio content over public IP networks.

SureStream enables you to:

a Save Money:

By replacing your synchronous or managed IP Links with the public internet, you can save up to 90% on the cost of your audio transport bills and generate a return on your investment in under 6 months!

b Deliver High Quality Audio:

The audio quality of your station should not be sacrificed for the sake of cost savings. SureStream enables you to maintain consistently high audio quality with no drop-outs and no jitter.

c Keep Delay Consistent

For professional audio delivery, it is not acceptable for the signal delay to vary or to drift. The ability to maintain the delay at a consistently low level is particularly useful for remote broadcast applications and local content insertion.

d Relax !

SureStream offers you the same level of uptime and reliability as a 'five nines' Telco service. You are protected not only from drop-outs and glitches but also from a complete loss of connection! With SureStream, the internet finally constitutes a viable alternative to existing synchronous networks such as T1, E1 and ISDN without any compromise to your station's sound.

SURESTREAM

Heard it All Before?

This may sound a little familar. There are others who claim to offer the same type of solution but SureStream takes a completely unique approach which combats ALL not just some of the issues of IP Networking. Watch out for the following methods that some manufacturers offer:

1 Bandwidth scaling

For some, ensuring continuity of service is the key aim so they employ schemes that scale-back the quality of the audio or adjust the delay depending on the availability of bandwidth or the performance of the link. This approach ensures delivery but sacrifices consistent audio quality and consistent delay. SureStream doesn't work like this!

Bandwidth Scaling
Sacrifices consistent audio quality

2 Link Switching

A different approach that some offer is called link switching – this is where a codec will monitor two separate links and automatically switch to the one offering the best link quality. However, this assumes that the past performance of the link is a suitable indicator of future performance and leaves the link vulnerable to a Loss of Connection at any point in the delivery. SureStream doesn't work like this!

Link Switching
Leaves the link vulnerable to a loss of connection

3 Variable Latency

Sometimes called Elastic Buffering, variable latency causes problems for remote broadcasts, as it will affect natural talk-back with the studio. It also makes it difficult to ensure the timing of local content insertion for studio to transmitter and audio distribution links. SureStream doesn't work like this either!

Variable Latency
Inconsistency problems with talk-back and content insertion

SureStream is unique in the market and, unlike the approaches mentioned; it does not compromise on any area.
It delivers:

- Robust and uninterrupted streaming
- Low and constant latency
- Consistently, High Audio Quality

All using standard IP links. And not just standard ADSL links but also wireless 3G and 4G, LAN, WAN and Wi-Fi too.

How does SureStream work?

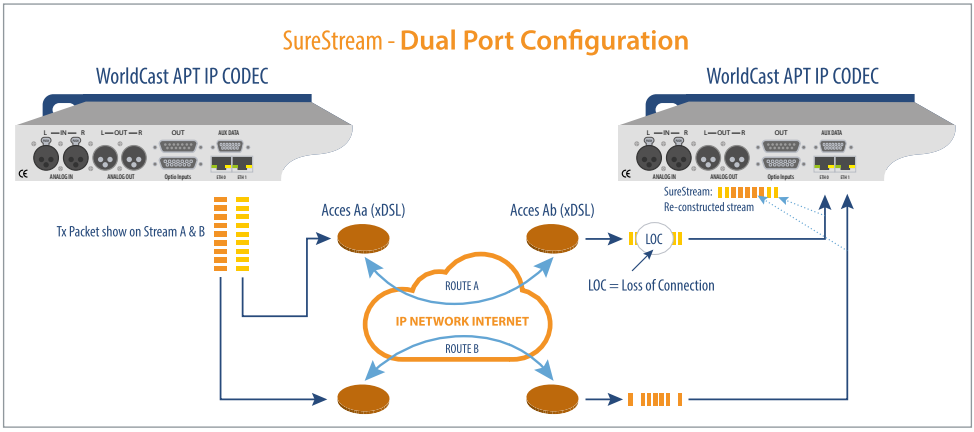
Well, firstly, SureStream capitalizes on the natural behavior of IP packets. The route of an IP packet is unpredictable and will depend on the routers and switches through which it passes. Therefore, if we send two streams from the same source to the same destination, they will travel in very different patterns, increasing the reliability and resistance of the system.

Sending duplicate streams is a good start but not good enough for the kind of perfection we are looking for! On the encoder side, SureStream employs a number of proprietary techniques that optimize the delivery of all streams throughout the network.

Then, it is on the receiving end where SureStream really works its magic! From the multiple streams received, APT's advanced resequencing engine produces one perfectly seamless, reconstructed stream. Perfect audio from an imperfect network!
In addition, SureStream allows you to configure a buffer level that will compensate for any jitter experienced. Once set, this delay is constant, enabling consistent playout.

Where can it be used?

SureStream works well on a single IP link for impromptu remotes or outside broadcasts but, for mission-critical studio transmitter links and audio contribution or distribution, we recommend utilizing two links from different providers to ensure optimum performance rivalling the 5 nine service offered by telcos. With two separate links, you are fully protected not only from network conditions but also any loss of connection.



The #1 Choice of Broadcasters for Audio over the Public Internet

SureStream gives you all the reliability and audio quality of a T1 using only cost-effective internet links. Hundreds of SureStream links are now active in the networks of Broadcasters throughout the US & worldwide.

To find out what SureStream can do for you, visit **www.surestream.ws** today!

"We haven't had a single lost audio packet or GPIO closure since we went live over 10 months ago and our network links are half the cost of a Point-to-point T1."

Andrew Stern
Cumulus San Francisco

"There are no audio drops from failover relays, glitches or other anomalies, as the SureStream decoder works its magic."

Larry Holtz,
All Classical Radio, Oregon

"SureStream technology has made possible something that was conventionally assumed to be impossible: having a high quality, real-time audio link over the open Internet."

Dan Houg, KAXE /
Northern CommunityRadio

WorldCast Systems > apt

contact@worldcastsystems.com
International Tel: +33 5 57 928 928
Americas Tel: +1 305 249 3110
www.worldcastsystems.com

Summary

It's been quite a journey over the past 13 years of IP Audio Codec development. We can conclude now that IP as a technology in broadcast is no longer new, it's no longer considered risky! The benefits from scalability to cost savings are well-known and accepted by most within the industry.

The applications to which we can apply IP Codec technology are without limits, from remotes to audio contribution and distribution and to STLs, all bases are covered. Consider the range of applications, the array of network types and the increasing speeds and availability of all sorts of IP connectivity and the broadcast engineer working in the field of Radio never had so many choices to get his audio from A to B and from A to B to Z !

However as we have outlined there are still challenges. You can negate these challenges by looking to an audio codec partner who works consultatively to guide you if you don't have the experience and who can look for solutions that can seamlessly adapt and protect the audio against the "unregulated" nature of many IP links. Consider pre-deployment planning and refer to our list of points for consideration in that section, this will help navigate you through the ever increasing options that are available.

Finally we hope you have found this significantly expanded audio primer useful and informative. As we stated at the beginning the ethos behind this booklet is to inform the broadcast professional from a wide perspective. Attempting to inform not only the engineer who has yet to deploy an IP Audio Codec but also those who are running AES67 Type environments and who have long migrated all codecs across to IP. Please retain this booklet as a handy reference tool and feel free to contact WorldCast Systems to discuss any projects or deployments you may have.

We'd love to help!

The WorldCast Systems Team

Authors

Kevin Campbell

APAC Americas APT Sales Director

Kevin Campbell has an accumulated 15 years' experience in Telco and Broadcast. Beginning as a network management engineer dealing with SDH, ATM and IP networks and moving into broadcast 12 years ago as customer support manager for APT WorldCast Systems codecs. For the past 11 years Campbell has worked in numerous commercial roles within APT WorldCast Systems, including European Sales Manager, VP Operations North America and in his current position as Sales Director APAC/Americas. During that time he has accumulated a wealth of experience on IP audio and codec based distribution projects across the world. In recent years he has delivered some of the largest IP Codec projects globally including a €750k USD project for NHK Japan to monitor the nationally strategic and important AM Transmitter network and a project of €500k in the US for the preeminent supplier of in-store music in the nation.

He has presented papers on audio coding and IP technologies globally at international conferences including NAB, NAB Radio, AES USA and AES Europe. Campbell is a graduate of the University of Strathclyde, Glasgow and a post-graduate of the University of Ulster, Belfast.

Kevin Campbell

campbell@worldcastsystems.com

Hartmut Foerster

Product Manager

Hartmut Foerster has been associated with APT WorldCast Systems since 1992 when he was appointed the first Master Distributor for audio codecs by the company in Germany and Austria. He pioneered the concept of the audio codec as a device to transmit professional and broadcast quality audio across telecommunications links and long distances on both ISDN and X.21. He also championed the Enhanced apt-X algorithm on the home territory of MPEG making the codec a defacto standard within significant parts of the ARD Group and the EBU. Since joining the company in 2004 he has marshalled the APT Codec range starting with the highly successful Oslo Multichannel codec and on to today's world leading NextGen IP Audio Codec solutions and the renowned SureStream technology. Foerster is a regular contributor to the EBU NACIP Forum working on codec interoperability and standards.

Hartmut Foerster

foerster@worldcastsystems.com

Tony Peterle

WorldCast Systems Inc Manager

Tony Peterle has been involved in broadcast across (so far) 5 decades, as an on-air talent and experienced chief engineer. Tony worked in markets in the Midwest, Hawaii, and the Pacific Northwest before joining Worldcast Systems in 2005. Originally a support contact for our US customers, Tony is now Manager of Worldcast Systems, Inc., and occasionally is called on to assist customers worldwide with pre-purchase, installation, and support issues on all of our product lines.

Tony has assisted in the deployment of many large monitoring and control networks with several topping the $500K mark, and the deployment of an AoIP codec network for a large supplier of Point of Sale music, a project that has surpassed $750k thus far. Tony has presented technical papers at numerous SBE chapter meetings, many SBE Ennes educational conferences, and has contributed a course on the use of SNMP for monitoring and control systems to the SBE University.

Tony has also been honored to present technical papers at Columbia University, the NAB Broadcast Technical Conferences, in many Latin American countries, and in 2014 to the IEEE Broadcast Technology Society

Tony Peterle

peterle@worldcastsystems.com

NOTES

WorldCast Systems

20, av Neil Armstrong
33700 Mérignac
Bordeaux-Métropole
France

+33 557 928 928
contact@worldcastsystems.com

UK Office

Whiterock Buisness Park
729 Springfield Road
Belfast, BT12 7FP
UK

+44 28 90 677 200
info@aptcodecs.com

WorldCast Systems Inc

19595 NE 10th Avenue Suite A
Miami, FL 33179
USA

+1 305 249 3110
ussales@worldcastsystems.com

10,00 €

www.worldcastsystems.com