AtlasIED APPLICATION NOTE

Public Address System Network Design Considerations

Background

AtlasIED provides network based Public Address Systems (PAS) that are deployed on a wide variety of networks at end user facilities worldwide. As such, a primary factor, directly impacting the reliability of the PAS, is a properly configured, reliable, well-performing network on which the PAS resides/functions.

AtlasIED relies solely upon the end user's network owner/manager for the design, provision, configuration and maintenance of the network, in a manner that enables proper PAS functionability/functionality. Should the network on which the PAS resides be improperly designed, configured, maintained, malfunctions or undergoes changes or modifications, impacts to the reliability, functionality or stability of the PAS can be expected, resulting in system anomalies that are outside the control of AtlasIED. In such instances, AtlasIED can be a resource to, and support the end user's network owner/manager in diagnosing the problems and restoring the PAS to a fully functioning and reliable state. However, for network related issues, AtlasIED would look to the end user to recover the costs associated with such activities.

While AtlasIED should not be expected to actually design a facility's network, nor make formal recommendations on specific network equipment to use, this application note provides factors to consider – best practices – when designing a network for public address equipment, along with some wisdom and possible pitfalls that have been gleaned from past experiences in deploying large scale systems.

This application note is divided into the following sections:

- **Local Network** – The network that typically hosts one announcement controller and its peripherals.
- **Inter-System Network** – The connections between Local Networks for transporting audio and control traffic.
- **Possible Pitfalls** – Problems previously encountered in system deployments.
- **Audio Technology Appendices** – Network information provided by the CobraNetand Dante technology vendors related to networks. Note, this is information availableas of the time of this writing. The CobraNet information is unlikely to be updated,but the reader should always be sure to check Audinate.com for the latest information on Dante network requirements, as this could evolve with time.

In this paper, "Local Network" refers to a LAN (Local Area Network) of switches possibly connected to other LANs and systems via Routers. A "Local Network" may also be implemented as a VLAN (Virtual LAN) which is carved out of a larger network.

Network requirements primarily depend on what technology is being employed for transporting audio over the network. As of this writing, there are three possible technologies used in AtlasIED products:

- **CobraNet** – Layer 2 isochronous audio transport licensed from Cirrus Logic
- **Dante** – Layer 2/3 audio transport licensed from Audinate
- **"IP Audio"** – Layer 3 audio portion of IEDnet+ used by such devices as Atlas IP Speakers.

The control protocols used are primarily IEDnet and some SNMP (Simple Network Management Protocol), both of which are UDP-based protocols. These protocols do not place any particular demands on a network like the audio transport protocols do. However, in some special situations, some of the IP audio devices may be deployed on a different subnet from the controller. In these situations, it may be necessary to enable IP-Directed Broadcasting in the network switches/routers. This is a feature that often is turned off by default on network devices.

Local Network

Local Networks will need to be designed to support one or more of the audio transport protocols identified above. In some installations, the network may be required to support two such protocols, such as CobraNet and IP Audio, or Dante and IP Audio. In designing networks it helps to understand basically what is happening with the protocols network-wise. The protocol network connections are summarized below. All public address system local networks should have layer 2 connectivity or the "equivalent" such as using L2TP (Layer 2 Tunneling Protocol) to achieve the same effect as one layer 2 network.

The general recommendation is to design the network to put one and only one announcement controller and its peripherals (i.e., one "system") on one local network. There are installations that work fine with two, three or more controllers/systems on the same local network. But, one must be careful to not have too many digital audio endpoints on the same local network (notes on this below).

Lifeline controllers must reside on the same layer 2 local network as the primary controller it is backing up. System designs that rely on one Lifeline to back up multiple primary controllers, means all those systems must be on the same local network (if audio device counts allow).

CobraNet uses layer 2 multicasting (not layer 3, like IGMP) for the clock master traffic (called the CobraNet Conductor Beat Packets), for endpoint notification/subscription traffic (called Reservation Packets), and for some audio when it needs to reach multiple endpoints. Many switches recognize this traffic as "broadcast" since the IG multicast/broadcast group address bit is set in the destination MAC addresses used, even though the destination MAC addresses are not all ff's. Beat packets occur at a rate of 750 times per second. Reservation Packets are at a much lower rate, each device sending out one such packet every 1 – 8 seconds, typically. When audio must be broadcast, those packets, too, are at a rate of 750/second.

CobraNet devices always connect to the network at 100 Mbps speed, but the port should be configured for auto-negotiate 10/100. (The auto-negotiation seems to be part of the way CobraNet determines that a port is "active".) There is an absolute upper limit of 255 CobraNet devices on one network, although performance issues have been seen when the count nears 200 devices.

Dante uses layer 3 multicasting (IGMP), but natively/unassisted can still only pass audio on a layer 2 local network. The timing is handled via the PTP (IED 1588, ver 1) protocol[1]. These multicast packets come at a rate of about 4 per second. Dante audio packets are generally either unicast or multicast at a rate of 3000 packets per second.

Some Dante devices (i.e., those based on the Ultimo chip) connect to a network at 100 Mbps. Other Dante devices can connect at gigabit speed (1000 Mbps). A good strategy might be to configure ports for auto-negotiate 100/1000. The upper limit of Dante devices on one local network depends upon which device is acting as the clock master. If it is a Brooklyn II based device, Audinate claims there is no upper limit, although testing may have only been done for up to around 300 devices. If an Ultimo chip is the clock master (because there are only Ultimo-based devices in the system), then the upper limit, as of this writing, is about 40 devices. Ultimos are used in many IED devices such as mic stations and all devices in the 5400 product line. Brooklyn II modules are used in the IP108-D/IP116-D and T112 products.

IP Audio uses layer 3 unicasting/multicasting (IGMP) on a layer 2 network. There are no timing/conductor packets and audio packets occur at a rate of 50 times per second. Most IP Audio devices connect to a network at a 100 Mbps rate. In some installations, it is necessary to configure QoS to prioritize the IP Audio packets (ports) to eliminate unacceptable jitter. IP Audio requires IGMP version 2 or higher support on the network.

When interfacing with a **VoIP/SIP** phone system, the network may also have to provide performance required by the VoIP PBX manufacturer.

Inter-System Network

For inter-system connections, a routed layer 3 connection is required for control (IEDnet). That is, the network should be designed with gateways (default routers) available on the local networks (LAN or VLAN) so that one IED controller can communicate with another. The bigger issue is how to transport audio from one local network to another. Again there are multiple options depending on system design needs/requirements.

CobraNet or Dante can be transported between local networks by using an IED1100DAB (Digital Audio Bridge) of the right variety. These units are available in CobraNet-to-CobraNet, Dante-to-Dante and CobraNet-to-Dante varieties. Each DAB has two sets of redundant network connections that are then connected on two different networks. In large system designs, with multiple announcement controllers, the second network connection on each system's DAB is connected to a "global network" (LAN/VLAN) that spans all systems. For example, when System A needs to send audio to System B, System A's DAB transports audio from A's local network to the global network and then System B's DAB transports the audio from the global network to B's local network. This is illustrated in the diagrams below.

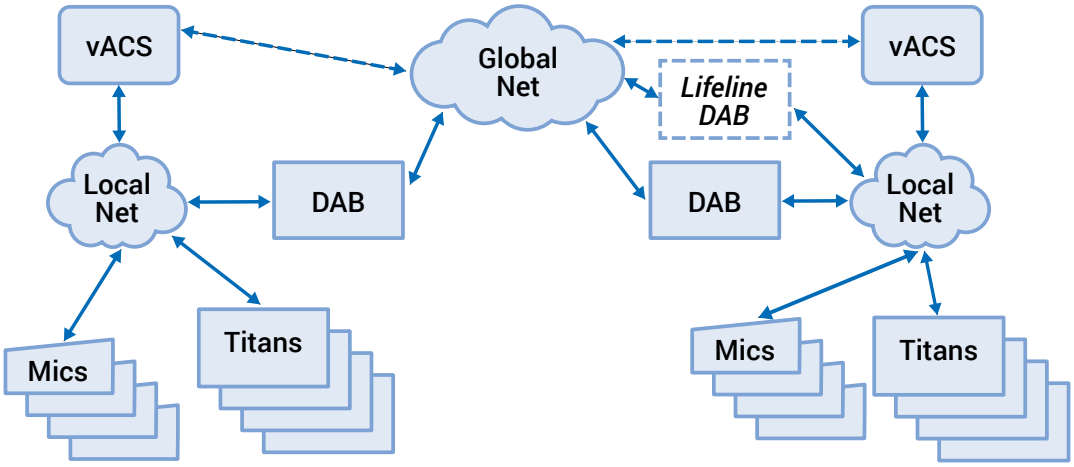
The advantage to transporting audio in this manner is that the audio latency end-to-end is low; lower than the human ear can perceive. So, if two system's zones are adjacent, no "echo" is heard when a user is standing between/straddling the zones. One additional requirement is that the global network is reachable (via gateway/router) by every system

[1] *Ver 1 is the older version of IEEE 1588 that does NOT require special switches. The newer Ver 2 of IEEE 1588 is required by other audio transports such as AES67 or AVB.*

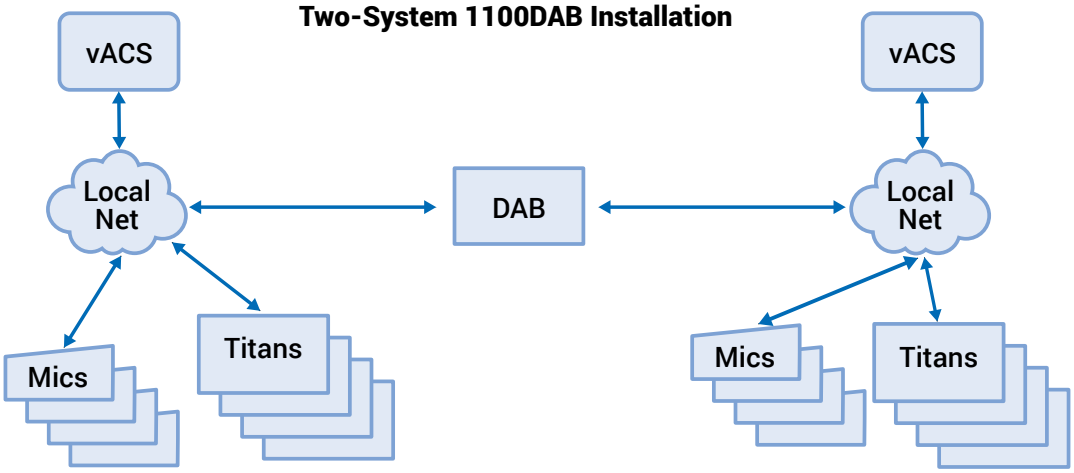
controller so these controllers can talk to the global network side of their DAB units, and properly configure the dynamic routing to other DAB units.

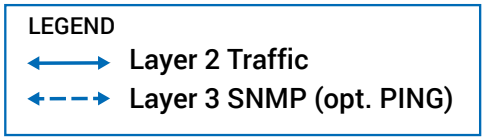
IEDnet+ (IP Audio) can be used when latency in the audio between systems is not an issue. This approach does *not* require additional equipment like DAB's nor a global network. This digital audio piggybacks on the same communication pathway (default gateway/router) used by the IEDnet control traffic. However, this may require special switch configuration to allow the audio to properly route. On some networks routed IP Audio requires Platform Independent Multicast (PIM) configuration which is dependent on the brand of switching gear. For example, Cisco routers require the configuration of Rendezvous Points.

Typical 1100DAB Installation



Two-System 1100DAB Installation





Possible Pitfalls

Below are some network design pitfalls that have been observed in previous deployments.

- **Broadcast Bandwidth Restrictions** – A feature on some switches is to put an upper limit on the broadcast traffic that can occur on a particular port. This is one measure that can be deployed to prevent the dreaded "broadcast storms" that can take down an entire network. As described above, CobraNet must broadcast some of its traffic, such as the conductor packets, and sometimes audio packets. On endpoints such as mic stations, this would mean a total broadcast bandwidth of under 2%, so, for example, a 10% Broadcast limit would not pose an issue. However, if that same rule is applied to a port on a sound card for controller or message server, or on up/down links between switches, it can result in many of the CobraNet packets being discarded. (Discarding beat packets causes distorted audio.)

- **Port Scanning the Audio Devices** – Port scanning software rapidly tests all possible network ports on all network devices. It has been found that running these scans on CobraNet devices can "hang" the device (cause it to go offline). There is one vulnerable UDP port on many devices. Plus, it has been found that the act of just scanning UDP ports very fast can overload the device's internal network stack and cause it to go offline. Therefore, it is recommended that this never be done on public address system devices. To ensure devices on the network are "safe", sample scans of representative devices may be done slowly. Most of the devices are not vulnerable to any kind of netbot take-over since firmware cannot be installed over the network. IED can work with local IT Security to identify devices that may be vulnerable (e.g., running some version of embedded Windows or Linux) if they wish to scan those devices. Note: As of this writing, port scan testing has not been evaluated on Dante or IP Audio devices, only CobraNet devices.

- **Restrict/Filter Multicast Addresses** – Some network ports may have filtering to remove multicast messages used by switches (e.g., Cisco) to check on health, backup pathways, etc. The multicast addresses used by Dante are close to these Cisco addresses, so if the filtering is too broad (e.g., 224.x.y.z) then Dante packets will be dropped as well on the port.

- **VLAN Tagging** – Support for this feature is turned off on all CobraNet network devices. That means, if the switches are not removing the tags themselves, the CobraNet devices will not properly process the packets (CobraNet or otherwise). Note: As of this writing, this has not been evaluated on Dante or IP Audio devices.

- **Not Having a Backup of the Switch Configuration** – It is always good practice to make backup of the switch configuration, especially before making changes to the network configuration. If PAS equipment begins to fail following network configuration changes, it is advised to restore switch configuration from the backup before troubleshooting of PAS equipment.

- **Not Having a Well Documented Network Topology** – It is always good practice to document the physical network topology. If PAS equipment begins to fail, following physical changes of the network topology, it is advised to restore network equipment to the last working physical topology, before troubleshooting of PAS equipment.

- **Network Monitoring Appliances/Packages** – In some environments, it is desirable to run network appliances or install network monitoring packages to continually scan the network for devices and their status/properties. In some cases, this practice has been found to cause glitches in the PAS operation and even cause some of the embedded devices to reset themselves due to the excessive, denial-of-service like network packet "pounding" these appliances/packages sometimes inflict on the PAS devices. For example, one of these appliances/packages may continually "walk the MIB tree" for every device, during which time its requests/responses are blocking normal PAS controller traffic from reaching or being handled by the device's microprocessor in a timely fashion. It is recommended that the PAS devices be excepted from such scanning, such as by blocking the IP address range used for the PAS devices in the monitoring appliance/package configuration.

Bottom Line: It is the PAS Announcement Controller's responsibility to supervise network devices such as mic stations and digital power amplifiers, and report any negative status as faults in the system. Additional network appliances/packages which are duplicating this supervision could potentially have a negative impact on device status and impair PAS system operations.

CobraNet Network Requirements

The table below is copied from www.cobranet.info . Note, the AtlasIED CobraNet devices are configured for the 5-1/3 msec latency option.

TABLE 1: COBRANET NETWORK PERFORMANCE REQUIREMENTS

PARAMETER	MAXIMUM	COMMENTS
Beat Packet Delay Variation	250µs	If delivery of beat packets periodically varies from the nominal delay by more than this value, then the Receivers may loose sample lock or fail to meet clock delivery specifications.
Forwarding Delay, 5-1/3ms latency	500µs	Forwarding delay is the sum of store forward, queuing and propagation delays. Forwarding delay includes delay variation - i.e. 150µs forwarding delay + 250µs delay variation = 400µs. Thus tolerance of forwarding delay is reduced in the presence of delay variation. When forwarding specification is exceeded, audio is delivered reliably with additional latency. rxDelay and rxMinDelay can be used to observe and control this adaptation to forwarding delay.
Forwarding Delay, 2-2/3ms latency	250µs	
Forwarding Delay, 1-1/3ms latency*	125µs	
Maximum Forwarding Delay	5000µs	Audio cannot be delivered at any latency with extreme forwarding delays.
Maximum Forwarding Delay Variation, 5-1/3ms latency	1000µs	Delay variation exceeding these specifications will result in unreliable audio transport due unstable rxDelay determination. In some cases this may be addressed through manual rxMinDelay setting.
Maximum Forwarding Delay Variation, 2-2/3ms latency	500µs	
Maximum Forwarding Delay Variation, 1-1/3ms latency*	250µs	

* *Store-forward delay on a 100Mbit Ethernet connection is 121µs (assuming maximum length packets). This forwarding delay specification is only achievable on an audio-only dedicated network. The lowest latency achievable with CobraNet on a non-dedicated network is 1-2/3ms (using the 1-1/3ms latency mode with an rxMinDelay setting of 0x40 to make receivers tolerant to queuing delays introduced by non-audio traffic).*

Dante Network Requirements

The information below comes from the www.Audinate.com website, some from an article entitled "So You Want to Add Dante to Your Network?". Other information below comes from the website's FAQ (Frequently Asked Questions) related to networking.

Basically, what you need to know is that Dante is all IP-based, and makes use of common IT standards. Each Dante device behaves much like any other network device you would already find on your network.
In order to make integration into an existing network easy, here are some of the things that Dante does:

- Dante uses DHCP for addressing when available, and will auto-assign an IP address if it is not, exactly like a PC or Mac.
  - Dante devices will continue to 'look' for DHCP even after auto-assigning an IP address.
  - Some (but not all) Dante devices allow the setting of static IP addresses.
- Dante implements IGMPv3/v2 to assist with multicast management.
  - Support for IGMP is not required in a network; it is in Dante to make integration into mixed-use networks simpler.
- Dante can make use of DiffServ QoS in the network. Dante will tag packets, and its tags can be integrated into an existing IT network QoS scheme:

Priority	Usage	DSCP Label	Hex	Decimal	Binary
High	Time critical PTP events	CS7	0x38	56	111000
Medium	Audio, PTP	EF	0x2E	46	101110
Low	(reserved)	CS1	0x08	8	001000
None	Other traffic	Best Effort	0x00	0	000000

  - QoS is only required for 100Mbps or mixed 1Gbps/100Mbps networks. It can be helpful on mixed-use networks. It is not required for dedicated, all gigabit, Dante-only networks. When used, it must be configured with strict priority.
  - Note that the QoS could be re-marked, provided that the PTP packets still receive high priority.

So that you know what to expect, here is the kind of network traffic you will be seeing on your network with Dante devices:

- Dante uses UDP for audio distribution, both unicast and multicast.
  - Bandwidth usage is about 6 Mbps per typical unicast audio flow (containing 4 channels and 16 audio samples per channel). Flows are pre-allocated a capacity of 4 channels

The samples-per-channel can vary between 4 and 64, depending on the latency setting of the device. For multicast flows, channels-per-flow can be varied from 1 to 8 channels per flow.

  - Multicast audio is always on UDP port 4321. Unicast audio ports come from a range: 14336 - 14600.
  - Audio traffic should not take up more than 70% of the bandwidth of any network link.
- mDNS and DNS-SD for discovery and enumeration of other Dante devices (including Dante Controller and Dante Virtual Soundcard).
  - This traffic is on 224.0.0.251:5353.
- Precision Time Protocol (PTP) for time synchronization.
  - This is generally a few small packets, a few times per second. This traffic is on 224.0.1.129 - 224.0.1.132 ports 319/320.
- Dante-specific monitoring traffic on multicast addresses 224.0.0.230 - 224.0.0.232:8700-8706.

Does Dante require special switches?

No. We strongly recommend that Gigabit switches be used due to the clear advantages in performance and scalability. Read up on Networks and Switches FAQs on www.Audinate.com for suggestions and requirements.

What is the minimum requirement for switches in a Dante network?

All Ethernet switches are capable of working with Dante. However, please be aware that there are some features on some kinds of switches that will allow you to build larger and more reliable Dante networks.
While Gigabit switches are recommended, 100Mbps switches may be used in limited scenarios.

- For channel counts of 32 or more, Gigabit switches are essential. QoS is required when using Dante in networks that have 100Mbps devices. QoS is also recommended for Gigabit switches on networks that share data with services other than Dante.
- For lower channel count (<32) applications, a 100Mbps switch may be used as long as it supports proper QoS, and QoS is active. The use of 100Mbps switches without QoS is not recommended or supported.

What features are important when purchasing a switch?

Dante makes use of standard Voice over IP (VoIP) Quality of Service (QoS) switch features, to prioritize clock sync and audio traffic over other network traffic. VoIP QoS features are available in a variety of inexpensive and enterprise Ethernet switches. Any switches with the following features should be appropriate for use with Dante:

- Gigabit ports for inter-switch connections
- Quality of Service (QoS) with 4 queues.
- Diffserv (DSCP) QoS, with strict priority
- A managed switch is also recommended, to provide detailed information about the operation of each network link: port speed, error counters, bandwidth used, etc.

Can I use switches with EEE (Energy Efficient Ethernet or 'Green Ethernet') in my Dante network?

Short answer: no.

EEE (Energy Efficient Ethernet) is a technology that reduces switch power consumption during periods of low network traffic. It is also sometimes known as Green Ethernet andIEEE802.3az. Although power management should be negotiated automatically in switches that support EEE, it is a relatively new technology, and some switches do not perform the negotiation properly. This may cause EEE to be enabled in Dante networks when it is not appropriate, resulting in poor synchronisation performance and occasional dropouts. One can download a list of incompatible, unmanaged switched with Energy Efficient Ethernet from www.Audinate.com,
Therefore we strongly recommend that:

- If you use managed switches, ensure that they allow EEE to be disabled. Make sure that EEE is disabled on all ports used for real-time Dante traffic.
- If you use unmanaged switches, do not use Ethernet switches that support the EEE function, because you cannot disable EEE operation in these switches.