



**Technical
Guide**

IP Technical Foundations for Intercom

March 8, 2024

Table of Contents

Introduction.....	1
HelixNet.....	2
LQ.....	4
V-Series Panels Over IP	6
Agent-IC.....	8
EHX Trunking	11
EHX E-Dante	15
Key Terms	18

Introduction

With a variety of intercom products operating in the IP domain, Clear-Com has many products including HelixNet partyline, LQ, Eclipse-HX panels, Eclipse-HX trunking, Eclipse- HX Dante integrations with outside resources, and Agent-IC mobile intercom.

This paper discusses network parameter settings and network management for configuring a successful implementation for each of these product categories.

HelixNet



Network Consideration

The HelixNet HMS-4X, HRM-4X, HKB-2X and HXII-BP uses a 100Mb NIC.

HelixNet V3 TCP/UDP

Port 655 TCP – Linking HMS-4X

Port 80 HTML – Core Configuration Manager

Port 6000 TCP – Pairing with HKB-2X, HRM-4X, and HXII-BP
Port 6001 TCP – Authenticate, update, reboot.

Port 5353 UDP - mDNS, Expansion, Pair/Link by Name, Port 6001 UDP – Audio

Managed Ethernet Switch

When connecting HelixNet to managed network switch ensure that the network ports are set to Auto-Negotiation or 100Mb full duplex.

If the system is using more than one switch the link between the switches should be set to auto-negotiation or both side of the link should have auto-negotiation off. One of the most common causes of performance issues on 10/100Mb Ethernet links occurs when one port on the link operates at half-duplex while the other port operates at full-duplex. This occurs when one or both ports on a link are reset and the auto-negotiation process does not result in both link partners having the same configuration. It also can occur when users reconfigure one side of a link and forget to reconfigure the other side.

HelixNet tags relevant packets at DSCP Decimal 34 (=AF41), Assured Forwarding (AF) beginning with version 4.2 and onwards. Previous versions used DSCP Decimal 46 (=EF) Expedited Forwarding.

Unmanaged Ethernet Switch

Since unmanaged Ethernet switches do not allow user manage port speeds, it is best to use a 10/100Mb switch.

If an unmanaged Ethernet switch is connected to a managed Ethernet switch, the port on the managed switch needs to be configured to 100Mb full duplex.

Hubs

Hubs should not be used with HelixNet, because when a hub receives a packet at one of its ports, it retransmits (repeats) the packet to all its ports. This means bandwidth is wasted because all traffic is sent to all ports.

HelixNet Pairing By Name

If a HKB-2X, HRM-4X, and HXII-BP pair to a system by name. The system uses mDNS to propagate HMS and HRM presence in a network. As a device populates its mDNS entry, it specifies an ID, an IP address, a name and a list of services.

When configuration changes, the mDNS entry is updated and all devices connected “by name” will update and re-pair/link/expand as required.

HelixNet Network Bandwidth

Audio is 300kbps per audio stream. Detailed breakdown of audio requirements is:

For example, two linked HMS, 10 HBP each, 3 HRM paired to HMS A and 5 HXII-BP paired over IP to HMS B.

Pressing All Talk on A sends out 1.2Mbps over IP from A (300kbps to each HRM and 300kbps to HMS B) and also 1.5 Mbps from HMS B (300kbps to each HXII-BP)

So the total IP bandwidth usage is proportional to the number of devices connected over IP.

LQ



LQ V3 TCP/UDP

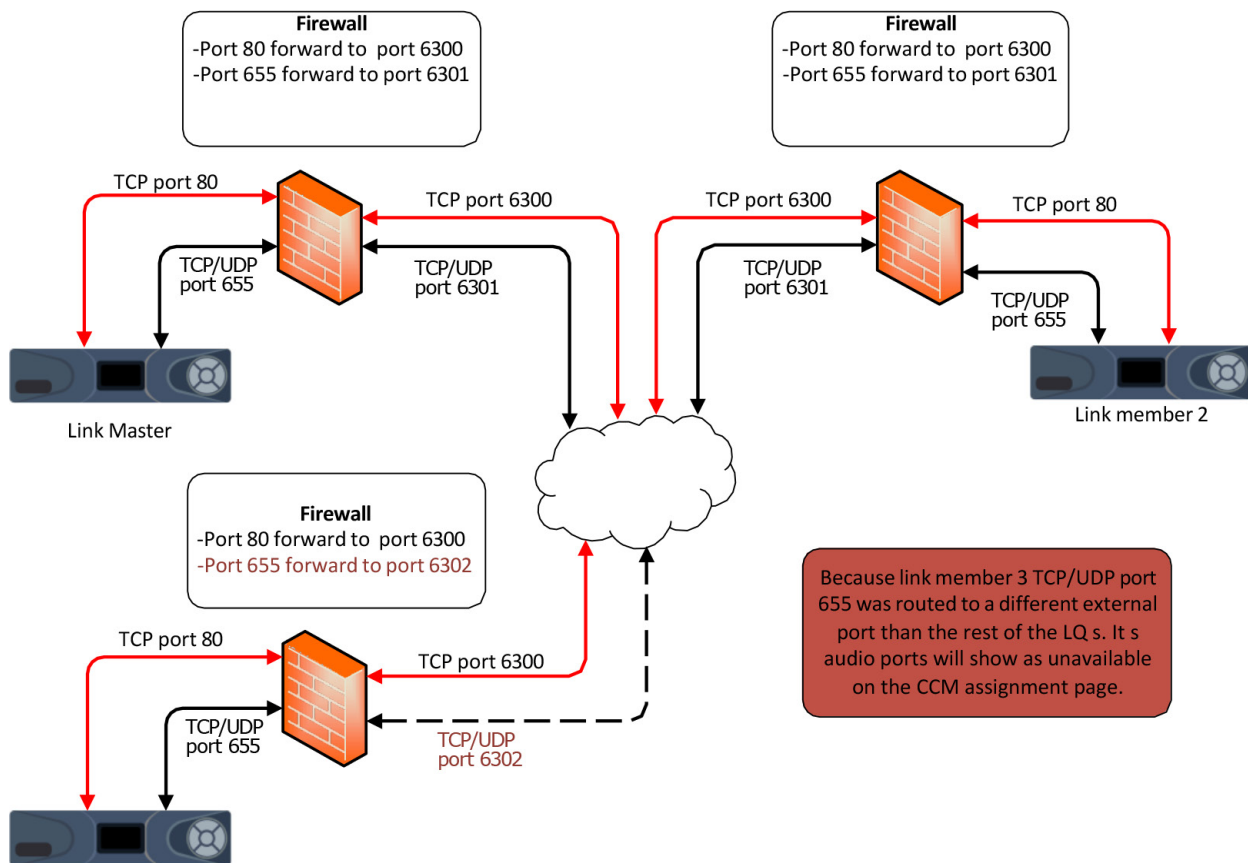
TCP port 80 is management (CCM)

TCP/UDP port 655 is the Audio/data

TCP/UDP port 6001 (IVC-32 card default port) Audio/data

Port Forwarding

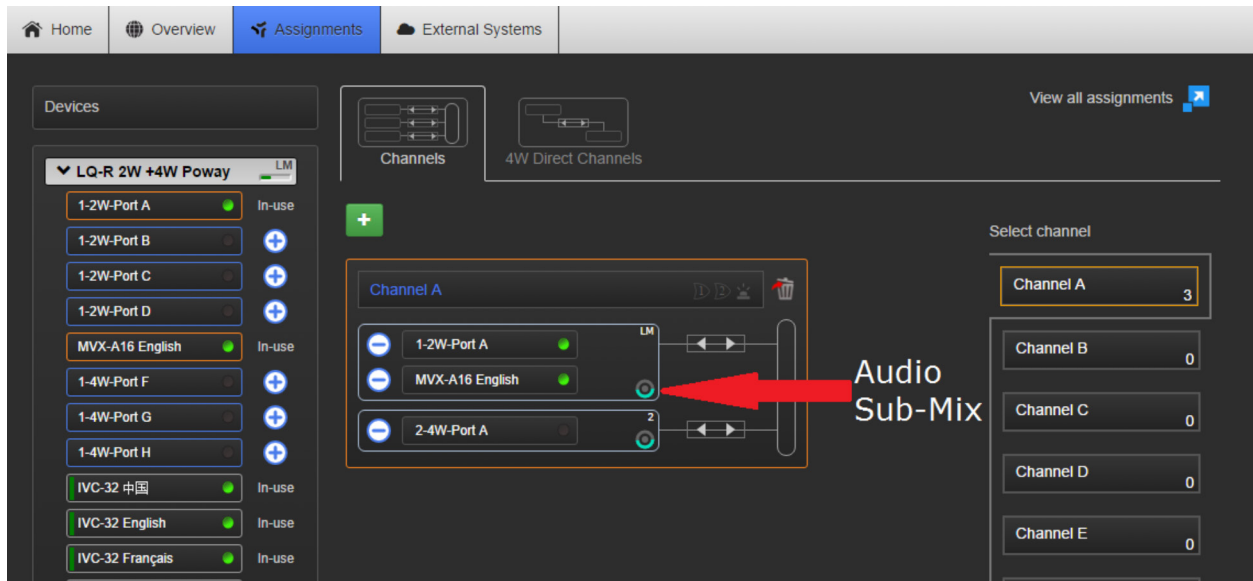
When LQ's are behind a fire wall you may need to route the external IP and ports (Internet connection) to the LQ's internal IP and ports (LAN). The port forwarding rules need to be the same for all the linked LQ's.



Silence Suppression

Silence Suppression is configurable for each audio sub-mix.

The Silence Suppression Algorithm continuously evaluates the average audio, and will only transmit when the mic audio is higher than the average audio level.



Note: Because the algorithm interprets constant audio as noise, audio from music or a noisy environment may be transmitted.

Bandwidth Requirements For Audio Data When Using IVC-32 Trunk


	LAN (kbps)	WAN (kbps)	Internet (kbps)
Half Duplex From IVC-32 to LQ Devices	120	90	140

Jitter Buffer

If the jitter gets too high, the panel starts to experience audio dropouts. The IP panels by default have three selectable jitter buffers:

- LAN mode panels can cope with jitter up to 80 milliseconds without audio dropout.
- WAN mode panels can cope with jitter up to 120 milliseconds without audio dropout.
- Internet mode panels can cope with jitter up to 200 milliseconds without audio dropout.

In EHX, customize LAN, WAN, and Internet jitter buffers by going to Preferences > IP Panels tab > deselect the Use defaults checkbox > enter the Min and Max jitter buffer values.



The screenshot shows the 'IP Panels' configuration page. Under the 'Jitter Buffer' section, there are three rows for LAN, WAN, and Internet. Each row has 'Min' and 'Max' input fields (both set to 0) and a checked 'Use defaults' checkbox.

V-series Panels Bandwidth

Bandwidth requirements for audio data when using IP Panels

	LAN (kbps)	WAN (kbps)	Internet (kbps)
Half Duplex From IVC32 to Panel	120	90	140
Half Duplex From Panel to IVC32	120	90	140**
Max Jitter Buffer (ms)	80	120	200

** **Note:** Silence suppression is enabled from Panel to Matrix, and Forward Error Correction module is ON both ways. The FEC module increases bandwidth but will support ~5% packet loss without affecting audio and keep acceptable audio up to ~10% loss.

Agent-IC Mobile Intercom



Agent IC TCP/UDP port

Port 6001 (default) TCP/UDP – TCP panel connection, UDP panel audio

Silence Suppression

Silence Suppression is always ON from Agent-IC to IVC32; only the Silence Suppression from the IVC to Agent IC is configurable.

The Silence Suppression Algorithm continuously evaluates the average audio on the Agent IC port, and will only transmit when the mic audio is higher than the average audio level.

***Note:** Because the algorithm interprets constant audio as noise, audio from music or a noisy environment may be transmitted to the device.*

VPN with Agent IC

If the IVC-32 card does not have access to an external IP address, a VPN can be used on the Agent IC device to connect to the IVC-32 card.

How to set up a VPN service on your iPhone or iPad (apple.com)

The easiest way to set up a VPN client on your iPhone or iPad is through an app like ExpressVPN, Tunnelbear, or Opera VPN. Download one of those great apps, install it on your iOS device, and open it.

After signing up or signing into your account, you'll be prompted to give permission to add a VPN configuration to your iPhone. Tap **Allow** to have the VPN configured on your iPhone automatically.

You'll then be prompted to enter your passcode or Touch ID to give permission to change your VPN settings. Enter your passcode, or activate Touch ID.

Once the VPN is enabled, you can select and connect it at any time without having to open the app again (use the app to change location and adjust other settings).

1. Launch **Settings** from your Home screen.
2. Select **General**.
3. Tap **VPN**.
4. If you have more than one, select the **VPN client** you want to use.
5. Toggle the **Status** switch on.

When you're done using the VPN, follow the instructions above to turn it off. Don't forget to turn it off, especially if you're on a free, limited plan.

How to manually configure a VPN on your iPhone or iPad

With your login information on-hand, you can manually configure a VPN client on your iPhone or iPad.

1. Launch **Settings** from your Home screen.
2. Select **General**.
3. Tap **VPN**.
4. Tap **Add VPN Configuration**.
5. Tap **Type**.
6. Select your **VPN type** from IKEv2, IPsec, or L2TP.
7. Tap **Add Configuration** in the upper left corner to go back to the previous screen.
8. Enter the **VPN settings information** including description, server, and remote ID.
9. Enter your **authentication login** including your username (or certificate), and password.
10. If you use a proxy, enable it by tapping **Manual** or **Auto**, depending on your preferences.
11. Tap **Done**.
12. Under VPN Configurations, toggle the **Status** switch on.

When you're done using the VPN, go to Settings > VPN to turn it off. To enable the VPN again in the future. Go to Settings > VPN and toggle the Status switch on.

Adding Android Nougat (android.com)

Use VPN in Android Nougat

First let us look at built-in VPN options within Android. The phone OS supports both L2TP and PPTP so will play nicely with most VPN services.

1. Navigate to **Settings, more under Wireless & Networks then VPN.**
2. Tap the '+' icon in the top right and add your VPN account details and Save.
3. **Connect to the VPN to test.** You will see a 'VPN activated' icon in your notification shade. Tap it to disconnect.

You can restrict all data use to a VPN if you use it a lot while on the move.

1. Navigate to **Settings, more under Wireless & Networks then VPN.**
2. Tap the **three-dot menu button** and select **Always-on VPN.**
3. Follow the wizard should one appear.

Opera Free VPN

Opera have offered a few VPN services to iOS users for a couple of months and now includes Android into the fold.

1. Navigate to the **Google Play Store** for the Opera Free VPN app.
2. **Download and install.**
3. Tap the **app icon**, agree the terms and allow it to use Android's VPN features.
4. Select a **server** and that's it.

Agent IC Network Bandwidth

	LAN (kbps)	WAN (kbps)	Internet (kbps)
Half Duplex from IVC-32 to Agent IC	120	90	140

EHX Trunking



EHX 9.0 TCP/UDP Ports For Trunking

- Port 1300 UDP – Matrix event log
- Port 42003 UDP – Map & Firmware download
- Port 42001 UDP\bc – Matrix to Matrix Comms
- Port 6001 (default) TCP\UDP – IVC-32 connect and audio

Intelligent Linking with trunks require all the connected frames are part of the same project. Intelligent linking dynamically allocates the available audio trunks as required when a talk or listen to another matrix system is requested. The Ethernet connection between matrices allows control data to route the audio lines so that any panel or interface on one matrix can communicate with panels or interface ports on the other matrices.

Intelligent Linking Over WAN

Frame status information needs to be transmitted from each frame to every other frame periodically. EHX system do not use true broadcast traffic i.e. destination address of packets being 255.255.255.255. Instead, network directed broadcast is always used when a single payload is to be directed to multiple other matrices, clients etc on the network. Network directed broadcast is where the packet address is the broadcast address for a specific network e.g. 192.168.1.255 on the 192.168.1.xxx (subnet mask 255.255.255.0) network.

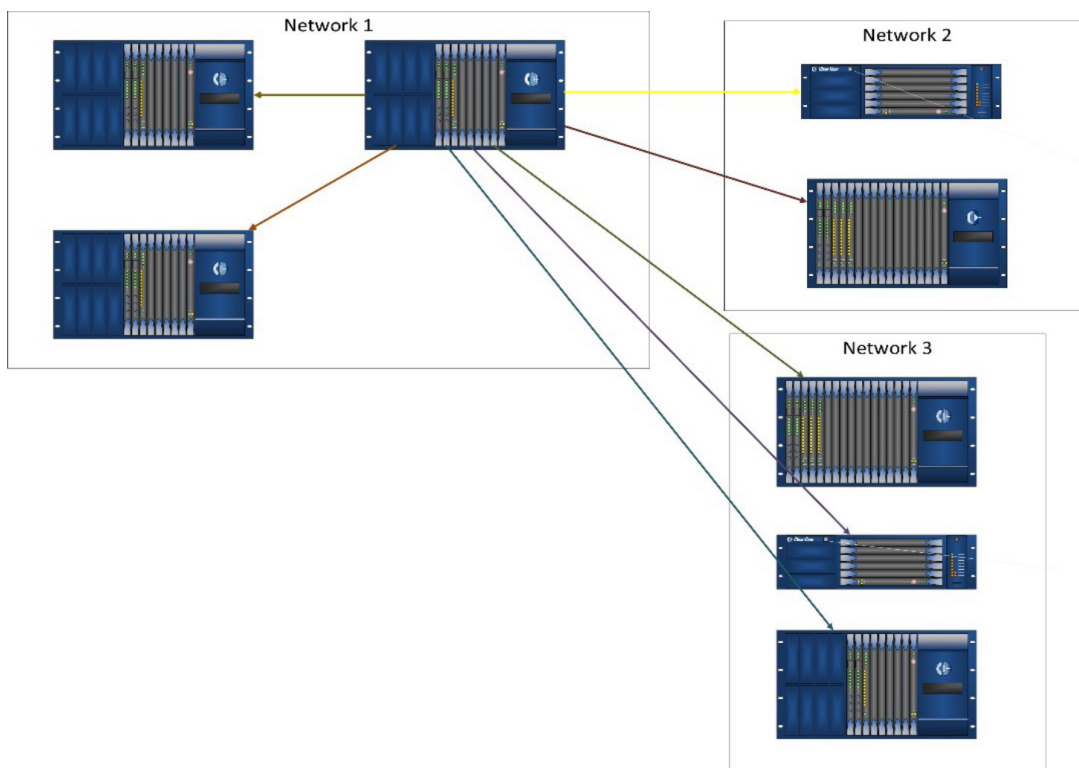
All unicast traffic will naturally cross between different LAN segments providing an appropriate default gateway has been set.

In order to optimize frame status traffic transmission in larger linked-sets the broadcast proxy feature was implemented as part of the EHX development.

From EHX 7.1 and above frames use a broadcast proxy mechanism in order to share their status with other frames.

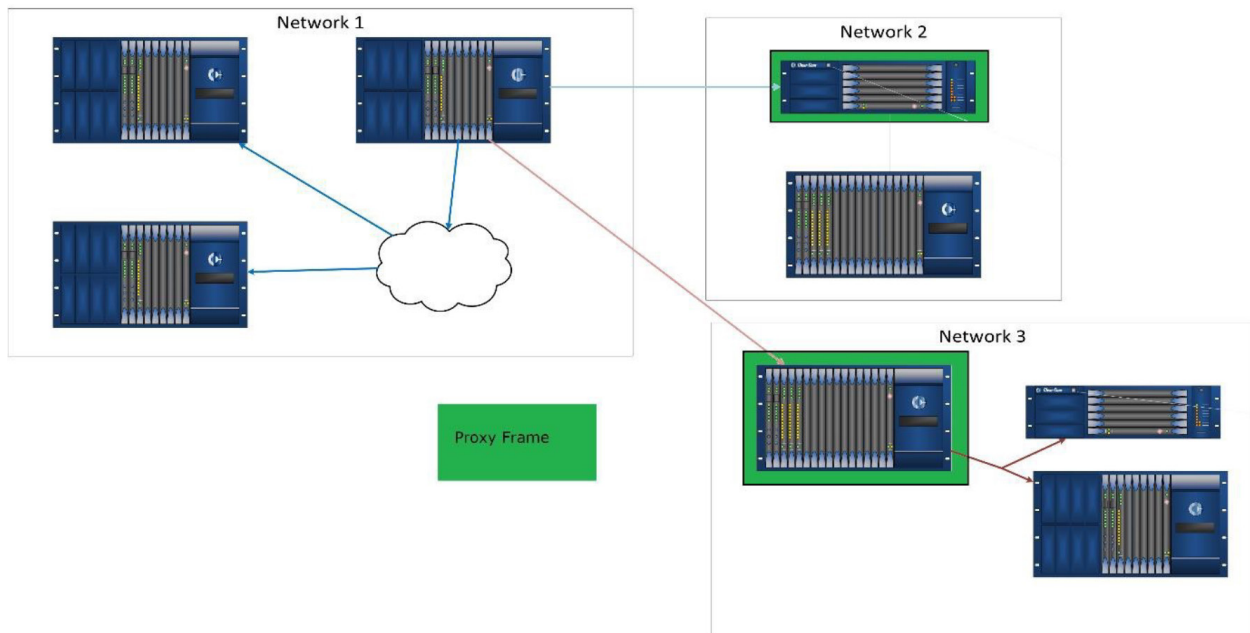
When a frame first initializes it will use unicast messaging to share its initial status with all other frames. Within this frame status each frame now additionally transmits its own subnet mask. Therefore, each frame now shares its network mask with all other frames, this allows each frame to gather a clear picture of the network topology of the linked-set.

Note: *The different colors are used below to show a different message transmission. However, each transmission is performed in order to transmit the same payload. Multiple messages are required in order guarantee successful transmission at this stage of the proxy mechanism initialization.*



Once a frame has ascertained the network topology of the linked-set it can group frames into networks (the subnet mask is required to establish this). Once any number of frames are established to be in a network, only one of the frames in the remote network will be sent the current frame status message. This message includes a parameter which instructs the receiving frame to broadcast this status on its own network as well as consuming the payload for its own use. For this transmission, this remote frame is the remote broadcast proxy for this remote LAN segment.

Note: The different colors are used below to show different message transmissions. Each transmission sends the same payload. When multiple arrows are with the same color then they are achieved by a single TCP/IP packet transmission.



Every time a frame sends out a status it picks a random (via random number generation) member of the remote LAN to act as its broadcast proxy. This is done to avoid single points of failure and to implement switchover type functionality for the proxy mechanism.

Frames on other LAN segments that are no longer seen to be transmitting will no longer be considered for use as the remote broadcast proxy. As soon as one of these frames re appears on the remote network it will be considered for use as a remote broadcast proxy on each transmit cycle.

If a frame receives a status message with the proxy forward parameter set then it resends the message to the network broadcast address of its own network. The 'from frame ID' field of the message is changed to look as though it came from the original frame and the proxy forward parameter is cleared from the message to stop subsequent retransmission.

The result of this feature is that the IP TX loading on frames can be greatly reduced as well as network traffic. This is because the source is no longer required to unicast its status to each remote frame.

Optimal Configuration

For best results, when there is some flexibility in the number of frames that can be placed on each LAN then evenly splitting the frames across two LANs gives the lowest loading on each frame that acts as a proxy.

The ideal situation is that all frames are configured to be on the same LAN segment. In this case no broadcast proxy mechanism is used. Instead, each frame reaches all other frames in the linked-set in the current transmission cycle by sending its payload in a single broadcast packet.

These network segments need to be configured using the conventional IP address, subnet mask and default gateway setting for the frame using EHX.

Redundant LAN

The redundant LAN feature is not supported when multiple LAN segments are being utilized on LAN 1.

This is because the redundant LAN feature uses intelligent selection of the LAN 1 or LAN 2 interface for the transmission of IP traffic based on packet destination address. The use of multiple LAN 1 segments (using default gateways) makes this network interface selection impossible as any IP would be reachable through either LAN interface.

When multiple LAN segments are in use on LAN 1 the redundant LAN must be not be enabled. This is done by leaving the frame secondary IP address set to the default of 255.255.255.255.

Intelligent Audio Trunk Line Port Priority

1. Fiber – these trunks are given top rating i.e. they are used whenever possible. This is because the fiber card only exists to trunk matrices together.
2. MADI, Dante – Low latency, linear audio.
3. E1/T1 – G722 or G711 compressed, low latency audio.
4. MVX – Low latency good quality audio, however, typically, link detection is not supported. No link detection when 4-wire cabling used. See appropriate manual for cabling that supports link detection.
5. IVC32 – These are given the lowest rating as they have lower audio quality and increased audio latency.

IVC-32 Trunking Bandwidth

	LAN (kbps)	WAN (kbps)	Internet (kbps)
Half Duplex from IVC-32 to IVC-32 Trunking	120	90	140

E-DANTE64-HX



E-Dante-HX Description

The E-DANTE64-HX card can operate in one of the multiple DANTE configurations, providing an Eclipse-HX with 16, 32 or 64 channels of low latency, high quality AoIP interconnect.

Additionally, it can support all of the standard sample frequencies for professional use, including the 96kHz/32-channel option for high quality audio.

Ethernet Switch

Most Ethernet switches are capable with Dante. However, the user should 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 some 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.**

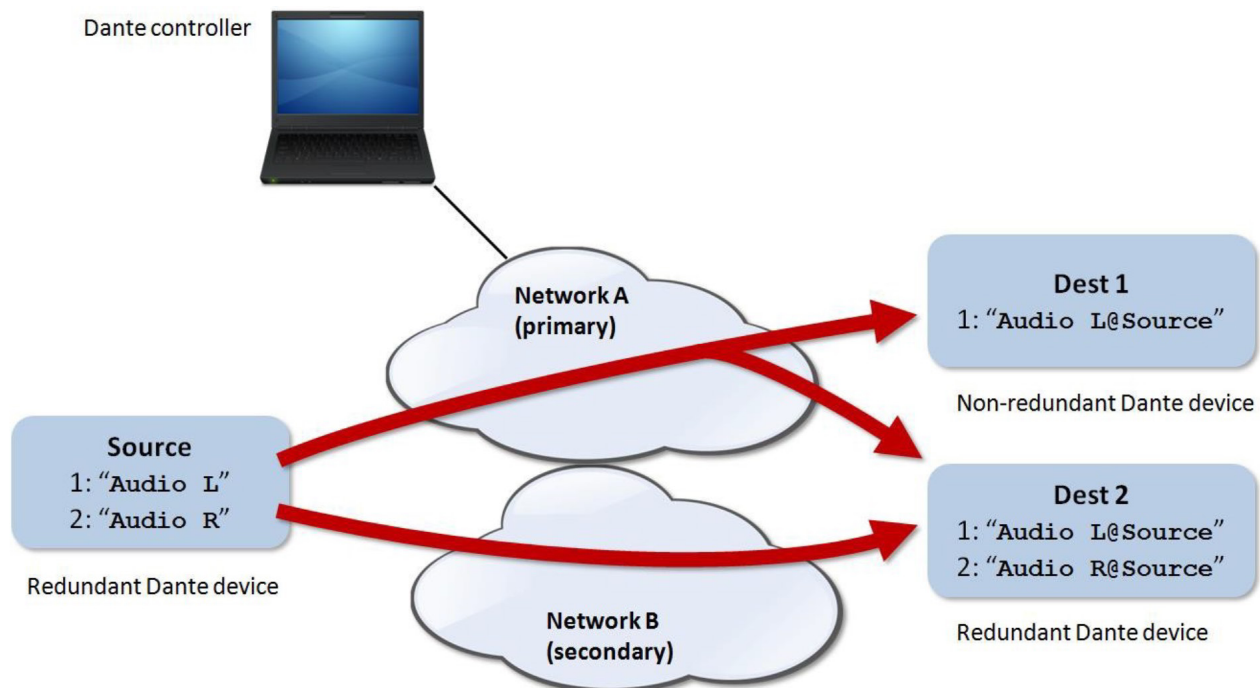
Any switches with the following features should be appropriate for use with Dante:

- Gigabit ports (or more) bandwidth for every port
- 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.
- 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.
- Fiber to Copper conversion preferably using the SFP/mini-GBIC form factor

Note: EEE refers to *Energy Efficient Ethernet* or 'Green Ethernet'

Dante Network Redundancy

The e-Dante card comes equipped with a Primary and secondary 100 Mbps/1 Gbs; auto-sensing NIC's. Primary interfaces should be connected to one physical network. If redundancy is being used, secondary interfaces should be connected to a second separate network. Secondary interfaces cannot communicate with primary interfaces. If the secondary network is connected to a device that supports redundancy, it is enabled automatically.



The same audio data is transmitted on both the primary and secondary networks simultaneously. In the event of a failure on one network, audio will continue to flow via the other network.

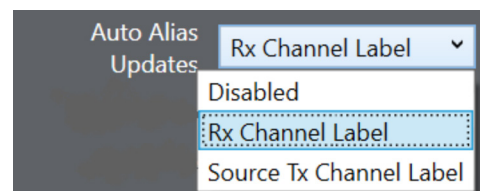
Note: Dante redundancy requires that both the primary and secondary interfaces on any redundant device are connected using the same link speed. For example, if the primary interface is connected to a 1 Gbps switch port, the secondary interface must also be connected to a 1 Gbps switch port. Similarly, if the primary interface is connected to a 100 Mbps switch port, the secondary interface must also be connected to a 100 Mbps switch port.

Dante Auto Alias Updates

Disabled – uses EHX Label

RX Channel Label – when selected any key for the Dante port will display the Dante controller receive channel label.

Source TX Channel Label – when selected any key for the Dante port will display the Dante transmit channel label of the routed source.



Note: RX Channel label will be used if no active subscription.

Key Terms

Internet Protocol (IP) – is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: Identifying hosts and providing a logical location service.

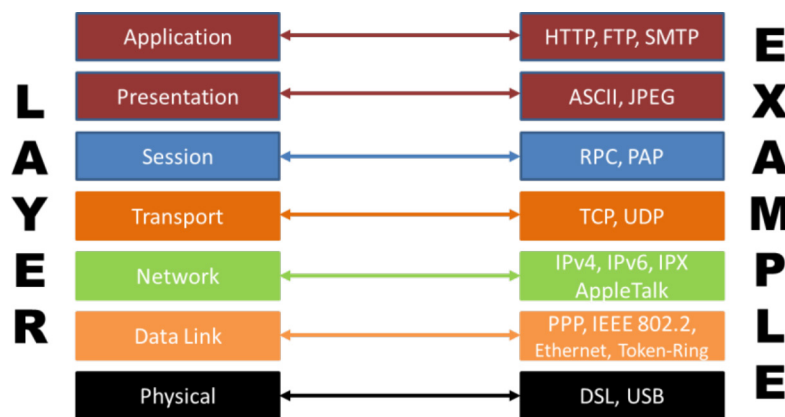
Transmission Control Protocol (TCP) – provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model.

User Datagram Protocol (UDP) – uses a simple connectionless transmission model with a minimum of protocol mechanism. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user’s program to any unreliability of the underlying network: there is no guarantee of delivery, ordering, or duplicate protection.

broadcast data (bc) – Directed broadcast packets NOT global broadcast packets which are 255.255.255.255

OSI 7-Layers – Reference Model is derived from ARPANET and initially financed by the Defense Advanced Research Projects Agency, or DARPA, of the US Department of Defense.

Note: *The OSI 7-Layer Model attempts to define how telecom and data systems should interconnect.*



Dynamic Host Configuration Protocol (DHCP) – dynamically distributes network configuration parameters, such as IP addresses, for interfaces and services.

Port Forwarding – is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

Virtual Private Network (VPN) – extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

Types:

Internet Protocol Security or IPSec – is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection.

Layer 2 Tunneling Protocol (L2TP) – or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection.

Point – to – Point Tunneling Protocol (PPTP) – creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

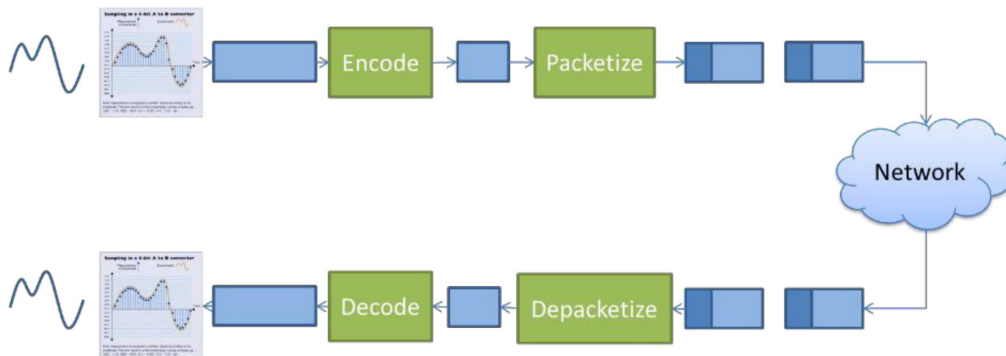
Secure Sockets Layer (SSL) and Transport Layer Security (TLS) – create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. SSL and TLS protocol is most commonly used by online shopping websites and service providers. Web browsers switch to SSL with ease and with almost no action required from the user, since web browsers come integrated with SSL and TLS. SSL connections have https in the beginning of the URL instead of http.

OpenVPN – is an open source VPN that is useful for creating Point-to-Point and Site-to-Site connections. It uses a custom security protocol based on SSL and TLS protocol.

Secure Shell (SSH) – creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

Quality of Service (QoS) – is the overall performance of the computer network, particularly the performance seen by the users of the network.

Codec – is a device or computer program for encoding or decoding a digital data stream or signal.



Bandwidth – is the bit-rate of available or consumed information capacity expressed typically in metric multiples of bits per second.

Jitter – is a common problem of the connectionless networks or packet switched networks. Because the information (voice packets) is divided into packets, each packet can travel by a different path from the sender to the receiver. When packets arrive at their intended destination in a different order than they were originally sent, the result is a call with poor or scrambled audio.

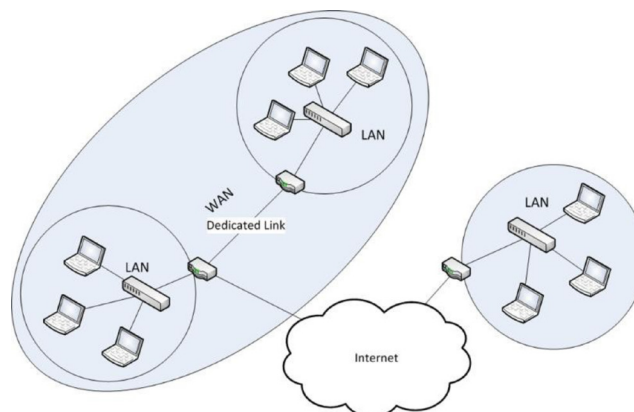
Dante – Based on industry standards, Audinate created Dante, an uncompressed, multi-channel digital media networking technology, with near-zero latency and synchronization.

For more training and information on Dante visit www.audinate.com/resources/training-and-tutorials

Local Area Network (LAN) – everything on the same segment using local sets of IP switches to local PCs and equipment.

Wide Area Network (WAN) – may contain several LANs connected over public networks (e.g. T1) or between sites through managed routers. The WAN may have a selection of QoS depending on priority, type of service and packet characteristics.

Internet – is an internationally connected network of billions of smaller WANs connecting businesses and homes.



Multicast – is group communication where information is addressed to a group of destination computers simultaneously. Group communication may either be application layer multicast or network assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission. Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group.

Internet Group Management Protocol (IGMP) / Snooping – is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

Broadcast – is the distribution of audio and/or video content or other messages to a dispersed audience via any electronic mass communications medium, but typically one using the electromagnetic spectrum (radio waves), in a one-to-many model.

Session Initiation Protocol (SIP) – is a communications protocol for signaling, for controlling multimedia communication sessions. Internet telephony, business IP telephone systems, service providers and all of the carriers use SIP. SIP can be used to set up and control voice and video calls, as well as instant messaging. The most common application of SIP is the setup and termination of Voice over IP (VoIP) telephone calls.

Voice over IP (VoIP) – is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

Real-time Transport Protocol (RTP) – is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features. RTP typically runs over UDP.

Auto-Negotiation – is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control.

Full-Duplex – both parties can communicate with each other simultaneously.

Network Interface Controller (NIC) – also known as a network interface card, network adapter, LAN adapter or physical network interface. Is a computer hardware component that connects a computer to a computer network.

Backplane Speed (aka: switching fabric or switching capacity) – Is the maximum number of packets/sec that can be routed out of any one port per second. When the forwarding capabilities of a backplane are greater than the sum of speeds of all ports (counted twice, Tx/Rx) we call the switching fabric non-blocking, meaning traffic between a pair of ports is not influenced by what traffic is exchanged on all other ports.

Forwarding Rate – The forwarding rate is expressed in packet per seconds and expresses how many packets per second are needed to reach a certain traffic volume (throughput). As forwarding rate depends on frame size, a switch is normally non-blocking up to a certain frame size.

Throughput – specifically relates to how much data can cross the switch in a given time frame.

SFP – The (Small Form-factor Pluggable) transceiver, also known as **mini-GBIC**, offers a standard, hot swappable electrical interface, one gigabit port that can support a wide range of physical media, from copper to long-wave single-mode optical fiber, at lengths of hundreds of kilometer



**Alameda, California, USA
Headquarters**

Tel: +1.510.337.6600

Email: MAGSales@clearcom.com

**Carlsbad, California, USA
Operations & Manufacturing**

Tel: +1.858.535.6000



www.clearcom.com