Network requirements specification for connection of NEO and NEO+ systems in multiservice networks.

Ref: D-0028084-EN-r2

Handbook

Content

1 INTRODUCTION

This document details the network specification for the interconnection of LDA Audio Tech PA/VA systems, specifically for the NEO and NEO+ families, as well as for the accessories that are typically integrated with these systems.

The network architecture will therefore depend on the number of NEO equipment or systems that are integrated. We divide it into two main parts:

1. Redundant ring of the evacuation system. In this area is the link between the NEO and NEXO units that form a closed redundant ring. This ring is managed by the system itself and as a general rule it must have a dedicated infrastructure. Fiber optic converters can be included if necessary.
2. Auxiliary multi-service network. In this part, the rest of the equipment that makes up the public address system will be installed, such as audio source injectors, microphones, management servers, etc. These devices connect to the system through the X-ports available on NEO units.

2 GENERAL SPECIFICATIONS FOR MULTI-SERVICE NETWORKS.

The general configuration required for the points of the service network where public address and voice evacuation system equipment is installed is described below.

The system uses two VLANs between all equipment. One dedicated to control and the other to ethernet/IP audio. Depending on the configuration of each device, each VLAN or both VLANs can be accessed separately (see 3.1).

The X ports of the ETX module can be configured in:

- Trunk mode (Flexnet), to have visibility to both control data and audio data on the same port.
- Untagged mode, to access a single VLAN on each port.

In both cases the speed is 100Mbits/s.

2.1 VLAN configuration and requirements

The traffic generated by the computers is detailed in the following sections. The general requirement is that the communication over these VLANs is **transparent**, allowing **broadcast and multicast Ethernet** communication between their endpoints regardless of the protocol. VLAN identifiers can be configured on the equipment to match those of the network if deemed necessary. This would be mandatory for Flexnet mode.

There are different protocols in the network infrastructure to extend VLANs in large IP networks. MPLS or similar routing systems may be used depending on the topology of the multi-service network used.

2.2 Security Settings. Best practices

The voice evacuation systems are based on the European EN54 family of fire regulations. These products are integrated into the Construction Products Directive, so they are required to be certified to higher standards than any general-purpose network infrastructure or multimedia device.

The building infrastructure and the ports connecting to the system must be provided with security measures that prevent access.

2.2.1 Physical access control

The safest method is to design a separate network with no physical access to any wiring terminal point where the system can be accessed via Ethernet connection.

2.2.2 Security Features in Ethernet Switches

The network infrastructure includes additional control measures that are used to secure access to systems, some of these measures are listed below. It should be noted that these measures are in addition to the others, and in many cases are not practical when applied in some systems. Comments from each one are included in relation to the needs or conflicts that they may generate with the NEO and NEO+ systems.

1. VLAN Privacy: Divides a network into VLANs and sub-VLANs to segment and isolate traffic between devices. It helps limit direct communication between devices on the same VLAN, improving security.
    a. It is an essential isolation method for controlling access points to the evacuation system.
    b. This document details the separation into VLANs required for the system.

2. MAC-based Access Control (PortSecurity): Allows you to define rules to control network traffic based on the MAC addresses that connect to each port.
    a. Each NEO and ZES device has 2 VLANs and 2 MAC addresses.
    b. A complete NEO system can exceed 100 MAC addresses on the same network port.
    c. Automatic use of this system is not recommended. The option to manually define addresses must be communicated in order to integrate an action protocol in the event of a replacement of equipment in the system.
    d. It is recommended to use notification mode instead of blocking MAC address changes
    e. The scope of action of this protocol only makes sense in the places of access

3. DHCP Snooping: Prevents DHCP attacks by monitoring DHCP messages and allowing only those from authorized DHCP servers. Prevents unauthorized devices from acting as DHCP servers.
    a. OK, no conflict.

4. IP Source Guard: Uses DHCP Snooping information to make sure that IP addresses on ports match authorized MAC addresses, preventing spoofing attacks.

   a. It could only generate conflict in the event of equipment replacement.

5. Dynamic ARP Inspection (DAI): Checks ARP packets to ensure they contain valid information, preventing ARP spoofing attacks.
   a. Ok, no conflict

6. Storm Control: Protects against broadcast, multicast, and unicast storms by limiting the amount of traffic that can pass through the switch. It helps prevent network congestion caused by attacks or misconfigurations.
   a. Ok. Just keep in mind that digital audio systems transfer a lot of multicast traffic and it should be allowed. Broadcast traffic is also transmitted between the system's equipment.

7. Access Control Lists: Filter traffic based on multiple layers of the OSI model (e.g., IP, protocol, TCP/UDP ports). They can be configured to allow or deny specific traffic, increasing security.
   a. Beware of protocol filters that may affect. See the traffic specifications in this document for more detail. The recommendation is not to activate filters within the evacuation system VLANs.

Protocols classified as unsafe:

There are lists of protocols that are currently considered insecure, for example, FTP, telnet, TFTP, SNMP. LDA Audio Tech does not use any of these protocols, but they are widely used in multiple industrial systems, so the recommendation for these cases is to separate the networks so that the traffic from the accessible points can never be mixed with the sensitive devices.

Most likely conflicts:

Port Security, DDos filtering and LLDP: Each ETX module computer integrates two different MAC addresses and a complete NEO system can integrate up to hundreds of MAC addresses through its X port. The traffic generated from each of these MAC addresses will change over time depending on the use of the system and its internal procedures at the level of monitoring, configuration, etc. For this reason, it is recommended to disable these protocols on those ports of the multiservice network since they can detect this traffic as undesirable. It is advisable to include an equivalent security countermeasure such as physical security control of ports accessible to the general public.

Audio **multicast traffic** can be of the unregistered type. Disable filtering for NEO and ZES22 VLAN ports. All interfaces are 100Mbits/s, so they cannot generate an overflow problem in the multiservice network.

Multicast L3/AES. In the **NEO+ audio VLAN,** the traffic is IP multicast.

It is recommended to enable IGMP to optimize the bandwidth used by the system.

2.3 Traffic Description

2.3.1 Audio VLAN

Audio packets have a special requirement of the low latency that they must meet to work properly. A packet is sent every 750us or 1 ms depending on the protocol.

The **CobraNet** protocol used in NEO and ZES22 operates at the data link layer, also known as the OSI layer 2 or link layer. It uses four types of packages.

All CobraNet packets are differentiated by a unique Ethernet Protocol Identifier (0x8819) assigned to Cirrus Logic. Because CobraNet is a local area network (LAN) technology and not a wide area network (WAN) technology, it does not use the Internet Protocol (IP) for audio transport.

The packets are multicast with target MAC 01:60:2b... and they must reach all the computers in the network, so it is necessary to have this type of traffic enabled.

The **AES67/Dante** protocol is used in NEO+, NEXO, EVACCore equipment.

The PTPv2 protocol is used for the synchronization of the devices at values of nanoseconds difference.

The audio is sent following the AES67 standard which uses IP multicast packets to transmit up to 8 channels of audio. In the standard configuration, each audio transmitter sends a packet every 1 millisecond.

In case of sending this traffic over shared networks, QoS and DSCP traffic priority mechanisms should be used.

2.3.2 VLAN de Control

The control data uses IP encapsulation with UDP protocol mainly. Depending on the type of communications, unicast, multicast or broadcast addressing will be used, so this type of traffic must be enabled within the virtual local network.

The traffic includes authentication mechanisms that should prevent any standard intrusion. In any case, fire regulations require physical access control to communication devices and ports.

2.3.3 Bandwidth

- Audio VLAN: Maximum usable bandwidth 100Mbit/s
- Control VLAN. Maximum bandwidth 10 Mbit/s

Package sizes. MTU

The maximum size that the data packet (MTU) can hold will be below 1,500 bytes.

2.3.4 QoS

Quality of service requirements for the correct transmission of Cobranet, NEO and ZES22 audio. The key requirement for sending high-quality audio in real time is system latency, because above a few milliseconds it is impossible to give live warnings by microphone. This means that the protocols have very restrictive requirements:

- <250 us. Maximum delay variation in synchronization packages. Target MAC: 01:60:2b:ff:ff:01
- <500us-1ms. Maximum end-to-end latency.

In systems where these specifications cannot be met, the
use of other topologies where these parameters are ensured. Our NEO and NEO+ systems will report failure in case the "Audio Link" requirements are not being met.

In case of mixing traffic in shared networks without VLAN. For systems with AES67, NEO+ and NEXO audio, it is recommended to configure the following settings:

- PTPv2 (Precision Time Protocol) → DSCP 56 (Expedited Forwarding - EF) traffic, prioritizing audio synchronization.
- Audio AES67 RTP (Real-Time Protocol) → DSCP 46 (Assured Forwarding - AF41), ensuring quality inaudio transmission.
- Control traffic → DSCP 00, ensuring correct communication between devices without interfering with audio streams.

3 CONFIGURING NETWORK PORTS

3.1 System devices. ETX Module

The equipment of the NEO, NEO+ system and the matrix ZES-22 use a communications module called ETX. It is a module that integrates an ethernet switch that connects and manages the two internal network cards, one for control data and the other for audio data. Therefore, two MAC addresses are available.

The module allows for various connection modes depending on the network topology used. The Flexnet mode will allow the communication of the audio and control data grouped in the same ethernet port within 2 VLANs (802.1Q). By default, the computers are configured with VLAN ID 1 for control and VLAN 2 for audio. These identifiers are configurable from the configuration software of each computer.

For more information, consult the user manuals of the equipment used in the system. You will find them on our Support Website

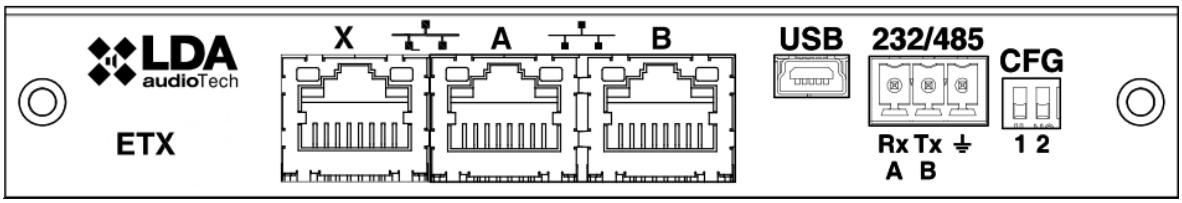

Illustration 1: ETX System Connection Bay

The module includes three ports (X, A and B) that can be configured to obtain control data and/or audio data. This will depend on the position of the CFG switch DIP according to the following table:

Brand	Description	Activation	
CFG	Port X: Flexnet* Port A: Control data only Port B: Audio Data Only	Position 00	
	Port X: Control Data Only Port A: Flexnet* Port B: Flexnet*	Position 01	
	Port X: Audio Data Only Port A: Flexnet* Port B: Flexnet*	Position 10	
	Port X: Flexnet* Port A: Flexnet* Port B: Flexnet*	Position 11	

Board 1: System connection configuration (*): Flexnet mode will have Control Data on VLAN1 + Audio Data on VLAN2

In the case of the NEO master, port B is usually in standby mode in modes 01, 10, and 11. This mouth will only open when a drop or disconnection occurs with other devices in the NEO system. It can cause Storm temporarily in case of intermittent errors.

As mentioned in previous sections, the ports of the equipment can manage the different VLANs, being able to establish the management of each one as follows (by default, VLAN 1 corresponds to control data and VLAN 2 is used for digital audio data, but it will be possible to customize it with the configuration software):

- **Control ports:** You must be untagged in VLAN 1 bind untagged mode, and not be a member of VLAN 2.
- **Digital Audio Port:** Must be untagged in VLAN 2 binding untagged mode, and not be a member of VLAN 1.
- **Flexnet port**: Must be tagged in trunk mode to VLAN 1 and 2. Both VLANs must be in tagged mode.