NEO+ and NEXO Network Requirements

Ref: D-0028084-EN-r3

Handbook

Content

1 INTRODUCTION

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

2 NETWORK ARCHITECTURE

Network architecture is divided into three main parts:

1. **Redundant ring** of the EN54-16 evacuation system. An area dedicated to the interconnection of NEO+ and NEXO units through a dedicated network infrastructure formed by the connections of the equipment itself. In distributed systems where a longer distance link is needed, a certified model of media converter is available for converting ethernet cable to fiber optic.

2. **EN54 Network** for interconnection between systems. NEO+ systems can be interconnected to form a larger system that can be managed from one or more general control points, which we call multi-site systems. The network linking NEO+ systems with evacuation microphones must be realized with switches that have been approved for the EN54 system. LDA Audio Tech's NEO+ system includes in its certificate an ethernet switch with redundant power supply.

3. **Auxiliary multi-service network**. For all other PA system devices, including PA microphones, audio players, AES67 or Dante equipment, and other devices attached to the system.

3 NETWORK SPECIFICATIONS.

NEO+ system equipment now operates with a simplified network configuration based on a single shared VLAN for audio and control IP traffic. This configuration allows greater flexibility in L3 networks and improves interoperability with modern systems. Bandwidth and security management is done through IP address segmentation.

NOTE: In previous versions of the NEO system, the systems operated under the FlexNet scheme of two VLANs, using one for control (VLAN 1) and one for audio (VLAN 2) integrated into the network through trunk mode ports. This configuration is still supported on NEO+ but is considered obsolete and cannot be used on systems that integrate NEXO or NEXO HUB outside of the redundant ring.

3.1 ETX NEO+ configuration

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

- Trunk mode (Flexnet), all audio and control traffic exits through the tagged formatted port for connection to switches.
- Untagged mode, traffic goes out without a tag to be accessible from any PC.
- When a single VLAN is used, audio and control traffic is accessible in ETX module modes 01 and 10.
  In both cases the speed is 100Mbits/s.

3.2 FlexNet VLANs Configuration and Requirements

The type of traffic generated by the devices is detailed in the following sections. The general requirement of **flexnet ring** traffic is that communication over this VLANs is **transparent**, allowing **Ethernet L2 broadcast and multicast** communication between its endpoints regardless of the protocol. In this way, the NEO and NEXO devices in the ring communicate correctly with 1 or 2 configured VLANs.

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.

4 Understanding ACSINet, AES67, and FlexNet+ Traffic

4.1 IP/AES67 audio traffic

Audio packets have a special low latency requirement that must be met to work properly, and an audio packet is sent every 1 ms.

The **AES67** compatible protocol is used on NEO+, NEXO, EVACCore equipment.

The traffic used is IP multicast that is directed to the receiving devices using intelligent network management.

4.1.1 IGMP Network Protocol

It is used for the coordination of multicast traffic over the network. The devices that want to receive traffic are subscribed and in this way the bandwidth is only used in the sections where there are registered receivers. It is essential to have the network correctly configured for this purpose.

To connect sections of Networks through Layer 3 routers, the PIM protocol will need to be activated between them, so that **IGMP** subscriptions can send traffic to devices connected at the network endpoints.

QoS and DSCP

Traffic is prioritized according to its latency needs by marking the **DSCP** field and activating **QoS** on the network. LDA AES67 traffic uses the value 46 for audio (high priority) and DSCP 56 for PTP (critical synchronization).

4.1.2 Protocols and IPs

PTPv2 for precision synchronization of devices at nanosecond differences. By default, it uses the IP 224.0.1.129

Discover v3 by LDA AudioTech. It uses a multicast IP address registered in IANA (224.0.2.11), to which all LDA devices subscribe via IGMP and thus facilitate the configuration of IPs without the need for DHCP.

IP Audio. 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. IP addresses are configured manually or chosen from the preconfigured list on the devices.

The address range is from 239.0.0.0 to 239.255.255.255. The document "ACSINet multicast IP Addressing" specifies the IP addresses used.

4.2 Traffic Control

The control data uses IP encapsulation with UDP protocol mainly. Depending on the type of communications, **unicast**, **multicast** or broadcast (Discover v1 only), addressing will be used so this type of traffic must be enabled within the virtual local network.

For the coordination of NEXO equipment in Domains or NEXO HUB in Cluster, the same protocols are used as in audio, so that the network configuration is exactly the same for both traffics. In this case, IP addresses are specific for control.

The traffic includes authentication mechanisms that should prevent any kind of interference between devices or intrusion issues. In any case, fire regulations require physical access control to communication devices and ports.

4.2.1 Bandwidth

- *Audio VLAN: Maximum usable bandwidth 100Mbit/s*
  - *Each 8-channel stream needs approximately 12Mbits/s*
- *Control VLAN. Maximum bandwidth 1 Mbit/s*

Package sizes. MTU

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

5 Network Security Settings. Best practices

The voice evacuation systems are based on the European EN54 family of standards for fire-fighting systems. These products are integrated within the scope of 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 EN54 system must be provided with security measures that prevent both physical and digital access.

5.1 Physical access control

The most secure method is to design a separate network with no physical access to any wired endpoints where the system can be accessed via IP Ethernet connection.

5.2 Security Features in Multiservice Networks

The network infrastructure includes additional control measures that are used to prevent unwanted access to systems, some of these measures are listed below. Observations are included in relation to the needs or conflicts that may arise with the NEO+ and NEXO Hub systems.

1. **VLAN Privacy**: Divide a network into VLANs and sub-VLANs to segment and isolate traffic between devices and systems that make it up. It helps limit direct communication between devices on the same network, improving security.
   - It is an essential isolation method for controlling access points to the evacuation system.
   - This document details the VLAN separation 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.
   - Each NEO+ device has 2 MAC addresses.
   - Each NEXO device has 1 MAC address.
   - A NEO+ system includes an internal loop that can exceed 100 MAC addresses on the same port of the multiservice network, and the NEO+ backup equipment will communicate these same MAC addresses if it goes into operation.
   - There may be conflicts with the automatic MAC detection system. In case of manually defining the allowed addresses, there must be a coordination protocol for cases where the replacement of system equipment is carried out. For this reason, it is recommended to use the notification mode instead of blocking MAC address changes.
   - The scope of action of this protocol only makes sense in places of public access without physical protection.
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.
4. **IP Source Guard**: Uses DHCP Snooping information to make sure that IP addresses on ports match authorized MAC addresses, preventing spoofing attacks.
   - 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.
    - 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.
    - Keep in mind that digital audio systems transfer a lot of multicast traffic and 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.
    - 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 with multi-service networks:

Port Security, DDos filtering and LLDP: Each device with ETX module 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 protection control of ports accessible to the general public.