# Especificación de requisitos de red para conexión de sistemas NEO y NEO+ en redes multiservicio.

Ref: D-028084-ES-r1

Handbook

# Contenido

# 1 INTRODUCCIÓN

Este documento detalla la especificación de red para la interconexión de sistemas de megafonía y evacuación de LDA Audio Tech, específicamente para las familias NEO y NEO+, así como para los accesorios que suelen integrarse con estos sistemas.

La arquitectura de red dependerá por tanto del número de equipos o sistemas NEO que se integren. La dividimos en dos partes principales:

1. Anillo redundante del sistema de evacuación. En esta zona se encuentra el enlace entre las unidades NEO y NEXO que forman un anillo redundante cerrado. Este anillo está gestionado por el propio sistema y como norma general debe disponer de una infraestructura dedicada. Se pueden incluir conversores a fibra óptica en caso necesario.
2. Red multiservicio auxiliar. En esta parte se instalarán el resto de equipos que conforman el sistema de megafonía, tales como inyectores de fuentes de audio, micrófonos, servidores de gestión, etc. Estos equipos se conectan al sistema a través de los puertos X disponibles en las unidades NEO.

# 2 ESPECIFICACIONES GENERALES PARA REDES MUTISERVICIO.

Se describe a continuación la configuración general necesaria para los puntos de la red de servicio donde se instalan equipos del sistema de megafonía y evacuación por voz.

El sistema utiliza dos VLANs entre todos los equipos. Una dedicada a control y otra a audio ethernet/IP. En función de la configuración de cada dispositivo se podrá acceder por separado a cada VLAN o a las dos a la vez (véase 3.1 ).

Los puertos X del módulo ETX pueden ser configurados en:

- Modo trunk (Flexnet), para tener visibilidad a ambos datos de control y datos de audio en un mismo puerto.
- Modo untagged, para tener acceso a una sola VLAN en cada puerto.

En ambos casos la velocidad es de 100Mbits/s.

## 2.1 Configuración y requisitos VLANs

El tráfico generado por los equipos se detalla en las secciones siguientes. El requisito general es que la comunicación sobre estas VLANs sea **transparente**, permitiendo la comunicación **broadcast y multicast Ethernet** entre sus extremos sea cual sea el protocolo. Los identificadores de las VLANs pueden ser configurados en los equipos para adecuarlos a las de la red si así se considerara. Esto sería obligatorio para el modo Flexnet.

Existen diferentes protocolos en la infraestructura de red para hacer extender VLANs en grandes redes IP. Se podrán utilizar sistemas de enrutamiento tipo MPLS o similar dependiendo de la topología de la red multiservicio empleada.

## 2.2 Configuración de Seguridad. Buenas prácticas

Los sistemas de evacuación por voz se basan en la familia de normativas anti-incendio europeas EN54. Estos productos se integran dentro de la directiva de productos para la construcción, por lo que se requiere que sean certificados bajo estándares más exigentes que cualquier dispositivo de infraestructura de red o multimedia de propósito general.

La infraestructura del edificio y los puertos de conexión al sistema deben estar provistos de unas medidas de seguridad que impidan el acceso.

### 2.2.1 Control de acceso físico

El método más seguro es diseñar una red independiente con imposibilidad de acceso físico a ningún punto terminal de cableado donde se pueda acceder al sistema mediante conexión Ethernet.

### 2.2.2 Funciones de Seguridad en Switches Ethernet

La infraestructura de red incluye medidas adicionales de control que se utilizan para securizar el acceso a los sistemas, algunas de estas medidas se listan a continuación. Se debe tener en cuenta que estas medidas son adicionales a las otras, y en muchos de los casos no son prácticas a la hora de aplicarlas en algunos sistemas. Se incluyen comentarios de cada uno en relación a las necesidades o conflictos que puedan generar con los sistemas NEO y NEO+.

1. Privacidad VLAN: Divide una red en VLAN y en sub-VLANs para segmentar y aislar el tráfico entre dispositivos. Ayuda a limitar la comunicación directa entre dispositivos en la misma VLAN, mejorando la seguridad.
    a. Es un método de aislamiento esencial para controlar los puntos de acceso al sistema de evacuación.
    b. Este documento detalla la separación en VLANs necesaria para el sistema.

2. Control de Acceso basado en MAC (PortSecurity): Permiten definir reglas para controlar el tráfico de red basado en las direcciones MAC que se conectan a cada puerto.
    a. Cada equipo NEO y ZES tiene 2 VLANs y 2 direcciones MACs.
    b. Un sistema completo NEO puede superar las 100 direcciones MACs en el mismo puerto de la red.
    c. No se recomienda el uso automático de este sistema. La opción de definir manualmente las direcciones debe comunicarse para integrar un protocolo de actuación en caso de sustitución de un equipo del sistema.
    d. Se recomienda el uso del modo de notificación en lugar de bloqueo ante cambios de direcciones MACs
    e. El ámbito de actuación de este protocolo sólo tiene sentido en los lugares acceso

3. DHCP Snooping: Previene ataques de DHCP mediante el monitoreo de mensajes DHCP y permitiendo solo aquellos de servidores DHCP autorizados. Evita que dispositivos no autorizados actúen como servidores DHCP.
    a. OK, ningún conflicto.

4. IP Source Guard: Utiliza la información del DHCP Snooping para asegurarse de que las direcciones IP en los puertos coincidan con las direcciones MAC autorizadas, previniendo ataques de spoofing.
    a. Sólo podría generar conflicto en caso de sustitución de equipos.

5. Dynamic ARP Inspection (DAI): Verifica los paquetes ARP para asegurarse de que contengan información válida, evitando ataques de ARP spoofing.
    a. Ok, ningún conflicto

6. Storm Control: Protege contra tormentas de broadcast, multicast, y unicast al limitar la cantidad de tráfico que puede atravesar el switch. Ayuda a prevenir la congestión de la red causada por ataques o configuraciones incorrectas.
    a. Ok. Sólo tener en cuenta que los sistemas de audio digital transfieren mucho tráfico multicast y debe estar permitido. También se transmite tráfico broadcast entre los equipos del sistema.

7. Access Control Lists: Filtran el tráfico basado en varias capas del modelo OSI (por ejemplo, IP, protocolo, puertos TCP/UDP). Pueden ser configuradas para permitir o denegar tráfico específico, aumentando la seguridad.
    a. Cuidado con los filtros de protocolos que puedan afectar. Ver las especificaciones de tráfico en este documento para más detalle. La recomendación es no activar filtros dentro de las VLANs del sistema de evacuación.

**Protocolos catalogados como inseguros:**

Existen listados de protocolos que se consideran inseguros actualmente, por ejemplo, FTP, telnet, TFTP, SNMP. LDA Audio Tech no usa ninguno de estos protocolos, pero sí que son ampliamente utilizados en múltiples sistemas industriales, por lo que la recomendación para estos casos es separar las redes de forma que el tráfico de los puntos accesibles no pueda nunca ser mezclado con los dispositivos sensibles.

**Conflictos más probables:**

Port Security, DDos filtering y LLDP: Cada equipo con módulo ETX integra dos direcciones MAC diferentes y un sistema NEO completo puede integrar hasta cientos de direcciones MAC a través de su puerto X. El tráfico generado desde cada una de estas direcciones MAC será cambiante en el tiempo dependiendo del uso del sistema y de sus procedimientos internos a nivel de monitorización, configuración, etc. Por esto se recomienda desactivar estos protocolos en esos puertos de la red multiservicio ya que pueden detectar como indeseable este tráfico. Es recomendable incluir una contramedida de seguridad equivalente como el control mediante protección física de los puertos accesibles por el público general.

El **tráfico multicast** de audio puede ser de tipo no registrado. Desactivar el filtrado para los puertos de las VLANs NEO y ZES22. Todos los interfaces son de 100Mbits/s, por lo que no pueden generar un problema de desbordamiento en la red multiservicio.

Multicast L3/AES. En la VLAN de audio de **NEO+** el tráfico es IP multicast.

Se recomienda activar IGMP para optimizar el ancho de banda empleado por el sistema.

## 2.3 Descripción del tráfico

### 2.3.1 VLAN de audio

Los paquetes de audio tienen como especial requisito la baja latencia que deben cumplir para funcionar correctamente. Se envía un paquete cada 750us o 1 ms dependiendo del protocolo.

El protocolo **CobraNet** usado en NEO y ZES22 opera en la capa de enlace de datos también conocida como capa de nivel 2 OSI o capa de enlace. Utiliza cuatro tipos de paquetes.

Todos los paquetes CobraNet se diferencian por un identificador de protocolo Ethernet único (0x8819) asignado a Cirrus Logic. Como CobraNet es una tecnología de red de área local (LAN) y no una tecnología de red de área amplia (WAN), no utiliza el Protocolo de Internet (IP) para el transporte de audio.

Los paquetes son multicast con MAC de destino 01:60:2b… y deben llegar a todos los equipos de la red, por ello se necesita tener habilitado este tipo de tráfico.

El protocolo **AES67/Dante** se usa en los equipos NEO+, NEXO, EVACCore.

Se utiliza el protocolo PTPv2 para la sincronización de los dispositivos a valores de nanosegundos de diferencia.

El audio se envía siguiendo el estándar AES67 que utiliza paquetes IP multicast para transmitir hasta 8 canales de audio. En la configuración estándar, cada transmisor de audio envía un paquete cada 1 milisegundo.

En caso de enviar este tráfico por redes compartidas se deberían emplear mecanismos de prioridad de tráfico QoS y DSCP.

### 2.3.2 VLAN de Control

Los datos de control utilizan encapsulado IP con protocolo UDP principalmente. Dependiendo del tipo de comunicaciones se utilizará direccionamiento unicast, multicast o broadcast, por lo que se debe dejar habilitado este tipo de tráfico dentro de la red local virtual.

El tráfico incluye mecanismos de autenticación que deberían evitar cualquier tipo de intrusión estándar. En cualquier caso, la normativa anti-incendios obliga a proveer de un control de acceso físico a los dispositivos y puertos de comunicación.

### 2.3.3 Ancho de banda

- VLAN de audio: Máximo ancho de banda utilizable 100Mbit/s
- VLAN de control. Máximo ancho de banda 10 Mbit/s

**Tamaño de paquetes. MTU**

El tamaño máximo que puede contener el paquete de datos (MTU) estará por debajo de los 1.500 bytes.

### 2.3.4 QoS

Requerimientos de calidad de servicio para la correcta transmisión de audio Cobranet, NEO y ZES22. El requisito clave para el envío de audio de alta calidad en tiempo real es la latencia del sistema, ya que por encima de unos pocos milisegundos es imposible dar avisos en directo por micrófono. Esto hace que los protocolos tengan unos requisitos muy restrictivos:

- <250 us. Máxima variación de delay en paquetes de sincronización. MAC de destino: 01:60:2b:ff:ff:01
- <500us-1ms. Latencia máxima end to end.

En sistemas donde no puedan cumplirse estas especificaciones se deberá contemplar el uso de otras topologías donde se aseguren estos parámetros. Nuestros sistemas NEO y NEO+ reportará fallo en caso de que no se estén cumpliendo los requisitos de “Audio Link”.

En caso de mezclar el tráfico en redes compartidas sin VLAN. Para los sistemas con audio AES67, NEO+ y NEXO se recomienda configurar los siguientes valores:

- DSCP EF (46) Clock traffic. Prioridad más alta (4)
- DSCP AF41 (34) Audio packets. Segunda prioridad (3)

# 3 CONFIGURACIÓN DE LOS PUERTOS DE RED

## 3.1 Dispositivos del sistema. Modulo ETX

Los equipos del sistema NEO, NEO+ y las matrices ZES-22 utilizan un módulo de comunicaciones denominado ETX. Se trata de módulo que integra un switch ethernet que conecta y gestiona las dos tarjetas de red internas, una para los datos de control y otra para los datos de audio. Por tanto, se disponen de dos direcciones MAC.

El módulo permite varios modos de conexión en función de la topología de red empleada. El modo Flexnet permitirá comunicar los datos de audio y de control agrupados en el mismo puerto ethernet dentro de 2 VLANs (802.1Q). Por defecto los equipos vienen configurados con el identificador de VLAN 1 para control y VLAN 2 para audio. Estos identificadores son configurables desde el software de configuración de cada equipo.

*Para más información, consultar los manuales de usuario de los equipos usados en el sistema. Los encontrará en nuestra Web de Soporte*

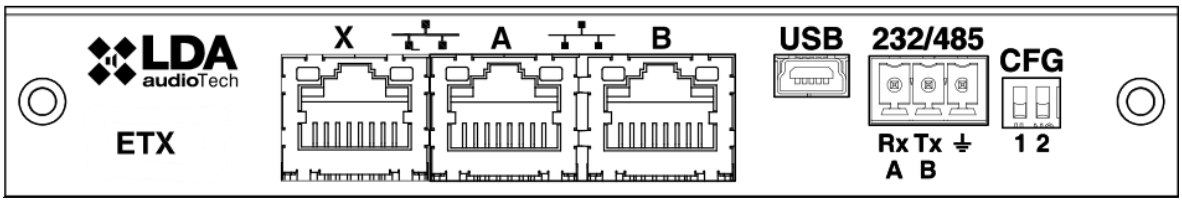



*Ilustración 1: Bahía ETX de conexión a sistema*

El módulo incluye tres puertos (X, A y B) que pueden ser configurados para obtener datos de control y/o datos de audio. Ello dependerá de la posición del DIP switch CFG según la siguiente tabla:

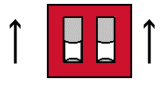
| Marca | Descripción | Activación | |
|---|---|---|---|
| CFG | Puerto X: Flexnet*<br>Puerto A: Datos de control exclusivamente<br>Puerto B: Datos de audio exclusivamente | Posición 00 |  |
| | Puerto X: Datos de control exclusivamente<br>Puerto A: Flexnet*<br>Puerto B: Flexnet* | Posición 01 |  |
| | Puerto X: Datos de audio exclusivamente<br>Puerto A: Flexnet*<br>Puerto B: Flexnet* | Posición 10 |  |
| | Puerto X: Flexnet*<br>Puerto A: Flexnet*<br>Puerto B: Flexnet* | Posición 11 |  |

*Tabla 1: Configuración conexión sistema*

(*): El modo Flexnet tendrá Datos de control en VLAN1 + Datos de audio en VLAN2

En el caso del NEO master, el puerto B suele estar en modo de espera en los modos 01, 10 y 11. Solo se abrirá esta boca cuando ocurra alguna caída o desconexión con otros dispositivos del sistema NEO. Puede provocar Storm temporalmente en caso de errores intermitentes.

Como se ha comentado en apartados anteriores, los puertos de los equipos pueden administrar las diferentes VLANs, pudiendo establecer la gestión de cada uno como sigue (por defecto, la VLAN 1 corresponde a datos de control y la VLAN 2 es utilizada para los datos de audio digital, pero será posible personalizarlo con el software de configuración):

- **Puertos de control:** debe estar sin etiquetar en el modo de acceso (untagged) de enlace a la VLAN 1, y no ser miembro de la VLAN 2.
- **Puerto de audio digital:** debe estar sin etiquetar en el modo de acceso (untagged) de enlace a la VLAN 2, y no ser miembro de la VLAN 1.
- **Puerto Flexnet**: deben etiquetarse en modo troncal (trunk) a VLAN 1 y 2. Ambas VLANs deben estar en modo tagged.