Application Note

Remote control of MXE5 with inter VLAN routing and ACLs

MXE Matrix Mix Engines are equipped with an OMNEO Dante OCA network interface for connecting to other systems, using CAT cables and Ethernet network switches.

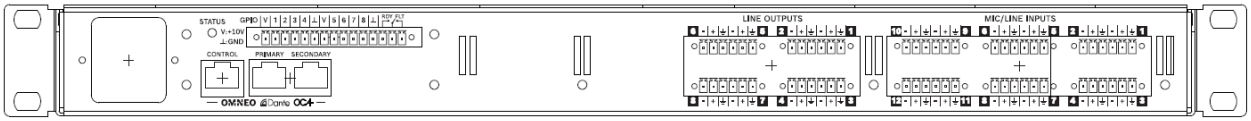


Image 1: MXE rear view

The network interface (*OMNEO Dante OCA*) can be found on the MXE's rear panel. It offers in total three network ports: *CONTROL*, *PRIMARY* and *SECONDARY*.

The three network ports can be configured via SONICUE to run either in Transparent, RSTP or Glitch-Free mode.

The *CONTROL* port always carries the same data as the *PRIMARY* port, except for Dante multicast audio traffic, which is filtered. This makes it ideal for connecting a WiFi access point, or generally pure control devices, but not for connecting it to a dedicated control VLAN (Virtual Local Area Network) – in this case it will act as a bridge(!) to the OMNEO/Dante network.

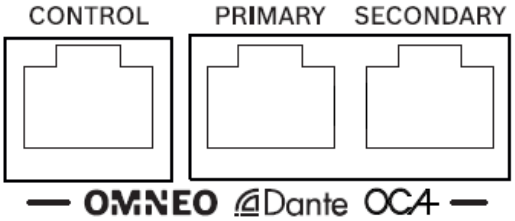


Image 2: MXE network interface detail view

OMNEO and network security

OMNEO offers a combination of audio and control data, providing numerous benefits. Efforts can be made to effectively manage and segregate audio and control data as needed for specific project requirements. For example, to keep an AV network structured and avoid interference with other systems, such as video, light or pay desk.

For security reasons, OMNEO devices should always be separated from the Internet (www) via a dedicated VLAN, and in addition be protected by an Access Control List (ACL).

This application note describes, with the example of an MXE5 matrix, Cisco CBS-350 switch and AVM FRTIZ!Box DSL router, how to isolate OMNEO devices via a separate VLAN, protecting it via ACL, and at the same time give control access from outside this secure "island".

For a full overview of possible network security measures for MXE and a connected SONICUE eco-system, please study the *MXE Security Precautions.pdf* (included in all SONICUE download packages).

Requirements for using SONICUE Control with MXE Control Server with fixed-IP and MXE with fixed ports:

MXE Matrix Mix Engine with firmware version 1.6.3342 (or higher)

SONICUE Sound System Software 1.4.0 (or higher) installed on computer

MXE Control Server

The MXE Matrix Mix Engine is the central device in the SONICUE eco-system, and thus requires special attention. It runs the Control Server, which translates the OCA commands -used for communication between OMNEO devices- to web-socket commands for communication with SONICUE control devices (such as WPN1 wall-panel, TPC-1, iOS devices and Windows PCs running the SONICUE Control app).

MXE Control Server – Ports

If an Access Control List (ACL) shall be configured, it's important to know which ports need to be allowed through the ACL:

- For Control Server communication MXE uses port 27999.
- For OCA communication MXE uses port 55555

The port 55555 is mainly relevant in combination with Crestron or Q-Sys controllers located in a separate VLAN, as the Crestron and Q-Sys plug-ins are based on the OCA protocol.

SONICUE ControlServer Discovery

By default, the SONICUE software and the SONICUE Control app find devices via mDNS and use device names for communication. The multicast IP address (224.0.0.251) used by mDNS is by definition of the IEEE not routable.

If control devices shall be separated from OMNEO/Dante devices via a dedicated control VLAN, the communication needs to be based on IP addresses and the network switch needs to support IP routing (Layer 3 mode).

SONICUE Panel Designer offers an option to define the *ControlServer Discovery* method.

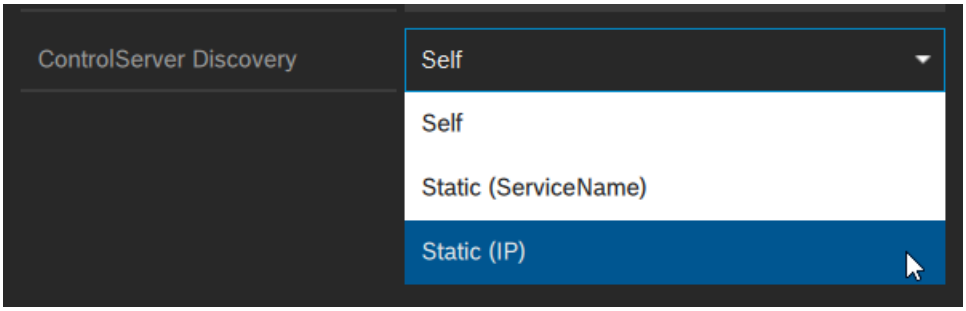


Image 3: SONICUE Panel Designer – *ControlServer Discovery*

By default, *ControlServer Discovery* is set to Auto or *Self* (depends on device), but it can be alternatively set to *Static (Service Name)* or *Static (IP)*.

The *Static (IP)* option must be used to separate SONICUE control devices, such as WPN1 wall-panel, TPC-1 touch panel, or iOS devices and Windows PCs running the SONICUE Control app, via a dedicated control VLAN from OMNEO devices such as MXE5 Matrix Mix Engines and a connected SONICUE eco-system.

For initial configuration all devices need to be in the same network as the PC running the SONICUE software for system design and configuration. After the control devices have received their desired configuration, they can be connected to a separate VLAN.

Test System for inter VLAN routing and ACLs

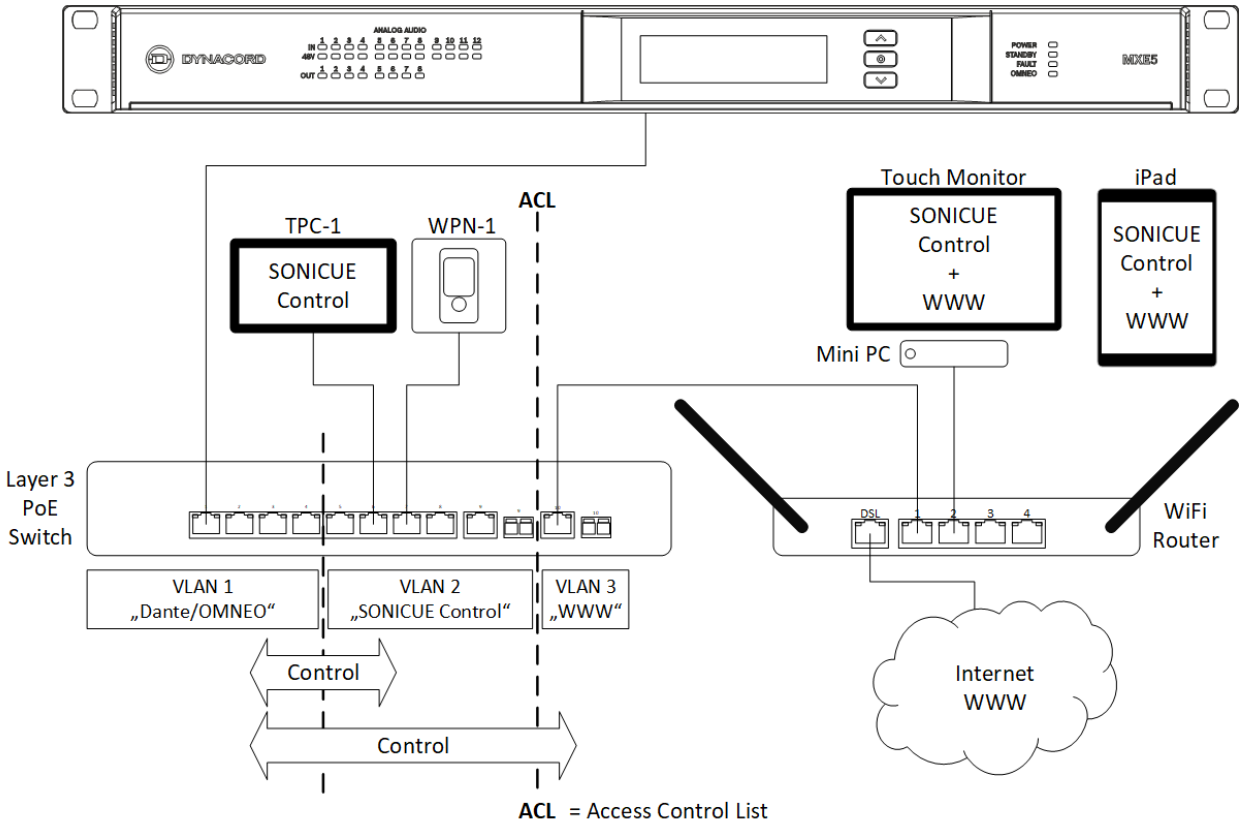


Image 4: Test System for inter VLAN routing and ACLs

Brief description of test system

The idea of this test system is to have all audio devices in one VLAN, and all control devices in (an) other VLAN(s).

- Audio exists only in VLAN 1.
- Control is routed to VLANs 2+3.

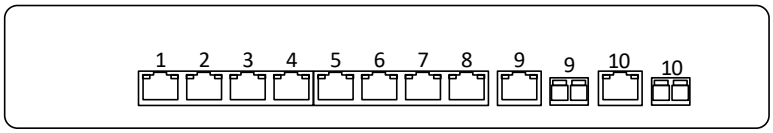
- VLAN 1 is used for all Dante and OMNEO devices with Dante audio.
- VLAN 2 is used for control devices that shall be separated from audio devices.
- VLAN 3 is used for control devices that shall be separated from audio devices and in addition shall have internet access.

The MXE control server will handle communication to control devices in VLAN 2+3 and serves as a „gateway“ to VLAN 1, where other OMNEO devices -like IPX or TGX amplifiers- can be connected.

IP addresses used in the test system

- VLAN 1
  - The MXE5 1 uses a fixed-IP 192.168.1.110 -> This is the Control Server
  - Other devices connected to VLAN 1 get their IP from VLAN 1 DHCP pool 192.168.1.1...100
- VLAN 2
  - The TPC-1 and WPN-1 get their IP from VLAN 2 DHCP pool 192.168.2.1...100
  - Other devices connected to VLAN 2 also get their IP from VLAN 2 DHCP pool
- VLAN 3
  - The WiFi Router uses a fixed-IP 192.168.178.1 -> This is the gateway to the Internet (www)
  - The iPad and mini-PC get their IP from the WiFi router DHCP pool 192.168.178.2...100
  - Other devices connected to VLAN 3/WiFi Router also get their IP from the WiFi Router DHCP pool

Switch configuration



VLAN 1 „Dante/OMNEO“	VLAN 2 „SONICUE Control“	VLAN 3 „WWW“

Image 5: PoE switch – VLAN networks

Switch used for testing: Cisco CBS350-8P-E-2G-EU (10 port, PoE)

- Basic OMNEO configuration (RSTP, QoS, EEE off, etc.)
- IP routing enabled (-> Layer 3 switch)
- VLANs
  - VLAN 1
    - Ports 1-4
    - IP interface 192.168.1.254/24 (this is also the gateway in VLAN 1)
    - DHCP pool 192.168.1.1...100/24
  - VLAN 2
    - Ports 5-9
    - IP interface 192.168.2.254/24 (this is also the gateway in VLAN 2)
    - DHCP pool 192.168.2.1...100/24
  - VLAN 3
    - Port 10
    - IP interface 192.168.178.254/24 (this is not the gateway in VLAN 3)
    - Gateway 192.168.178.1
- Access Control List (ACL)
  - ACE (ACL Extended)
    - Priority 10 Permit TCP from IP 192.168.1.110, wildcard 0.0.0.0, Port 27999 to 192.168.178.1, wildcard 0.0.0.255 (= from MXE with fixed-IP to any IP in Router network 192.168.178.1/24)
    - Priority 20 Permit TCP from 192.168.178.1 wildcard 0.0.0.255 to IP 192.168.1.110, wildcard 0.0.0.0, Port 27999 (= from any IP in Router network 192.168.178.1/24 to MXE with fixed-IP)
    - Deny any (exists at the end of an ACE by default, blocks any other traffic)
  - ACL binding
    - to interface 10 (port 10)
    - as IN and OUT
  - MXE5 ports to be permitted:
    - 27999 for MXE control via Control Server
    - 55555 for MXE control via OCA protocol (not used in test system)

WiFi router configuration

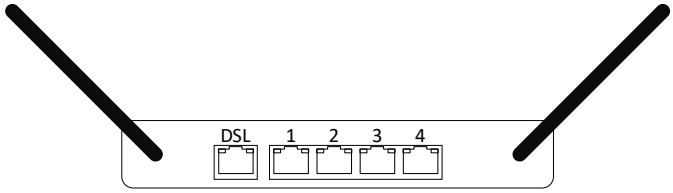


Image 6: WiFi router

WiFi routers used for testing: AVM FRITZ!Box 7530 and AVM FRITZ!Box 6820 LTE

- Default configuration:
  - IP address 192.168.178.1/24
  - DHCP pool 192.168.178.2...100/24

- Configuration to be made by user:
  - Static route 1:
    - Network 192.168.1.0/24
    - Gateway 192.168.178.254
  - Static route 2 (optional):
    - Network 192.168.2.0/24
    - Gateway 192.168.178.254
    - Only needed if there are devices to be controlled in VLAN 2

Third party product disclaimer:

Dynacord does not take responsibility for the warranty, quality, or availability of Cisco and AVM products. The Cisco and AVM products contained within this document were tested successfully at the time of publication. However, Dynacord cannot guarantee the compatibility with future models or variations of Cisco and AVM products, as these may not be compatible. Please refer to the Cisco and AVM website for product specific information.