MediaMatrix®

A Division of Peavey Electronics Corporation

CobraNet®

CobraNet Networking Guide

Version 2.0.0.0

July 7, 2017

Copyright notice

Email:*mmtechsupport@peavey.com* (*mailto:mmtechsupport@peavey.com*).

Scope

This guide is designed to help you understand the considerations when using MediaMatrix products on CobraNet networks. It is important that it is read and understood by network designers and systems administrators.

Contents

Chapter 1

Basics

In This Chapter

Introduction

A typical MediaMatrix installation will include two separate networks: the *control network* and the *audio network*.

The control network connects hardware devices, such as NIONs and nControls, with NWare, to allow control and monitoring using an NWare project.

The audio network allows digital audio data to flow between hardware devices using the CobraNet protocol.

The diagram below shows an example set up.

The control network and CobraNet network are both represented by a single *cloud*. You may choose to physically separate the wiring for the two networks, or logically separate the traffic using VLANs.

The NWare PC and NION are both connected to the control network. This allows the system administrator to configure the NION and use it in an NWare project. The CAB 4n does not have a direct connection to the control network, but it is still configured using NWare. Control data is passed to the CAB across the CobraNet network, via the NION.

Multicast traffic

MediaMatrix products communicate and discover one another by utilizing multicast health and discovery packets. The transmission of this multicast traffic is critical to the operation of the system and *must not* be impeded. No multicast traffic blocking is acceptable.

Even though the multicast traffic comprises a large number of packets, the total volume of data is small because each packet is very small. Expect to see a large number of multicast packets when monitoring network traffic while a MediaMatrix system is being used, but notice that the actual amount of data is minimal.

This multicast traffic is absolutely critical to the successful operation of the system so there must be no other traffic on the network with a higher priority or higher quality of service.

Network Ports for the control network

Different types of network activities on the control network require particular ports to be open. Make sure that the required ports are open for the types of activities you are expecting.

Network activity	Port number(s) required
Copying of audio files to and from MediaMatrix devices using FTP.	20 and 21
Web access using HTTP.	80
Controlling and monitoring devices using SNMP.	161
System health packet transmission. These packets are sent ten times a second by nControls, nTouch 180s and NIONs, and are received by all devices subscribed to the multicast address 239.0.0.10:1234. **Note:** These packets are very small and are not aggregated into a significant amount of network traffic.	1234
Controlling devices from an external program using RATC.	1632
Pandad communication across subnets. For more information, see Linking instances of Pandad across subnets.	4000
Discovery packet transmission. These packets are sent once every five seconds by nControls, nTouch 180s and NIONs, and are received by all devices subscribed to the multicast address 239.0.0.10:4321. **Note:** These packets are very small and are not aggregated into a significant amount of network traffic.	4321
Kiosk2Go websocket communications.	TCP port 7681

Kiosk2Go discovery application running on *iOS* (*https://itunes.apple.com/gb/app/kiosk2go/id916717124?mt=8*) and *Android* (*https://play.google.com/store/apps/details?id=com.peavey.kiosk2go&hl=en_GB*).	UDP port 7681

Opening a port in Windows Firewall

For Windows 7 users

1. Click the **Start** button.
2. In the **Search** box, type firewall.
3. In the results list, click **Windows Firewall with Advanced Security**.

   The **Windows Firewall with Advanced Security** dialog box is displayed.
4. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
5. In the left pane, click **Inbound Rules**, and then, in the right pane, click **New Rule**.
6. Follow the instructions in the **New Inbound Rule** wizard.

For Windows Vista users

1. Click **Start**, and then click **Control Panel**.
2. Click **Security**, and then click **Windows Firewall**.
3. Click **Allow a program through Windows Firewall**.
4. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
5. Click **Add port**.
6. In the **Name** box, type a name that will help you remember what the port is used for.
7. In the **Port number** box, type the port number.
8. Click **TCP** or **UDP**, depending on the protocol.
9. To change scope for the port, click **Change scope**, and then click the option that you want to use.

   The term *Scope* refers to the set of computers that can use this port opening.

For Windows XP users

1. Click **Start**, and then click **My Network Places**.
2. Under **Network Tasks**, click **View Network Connections**.
3. Right-click the connection that you use for the Internet, and then click **Properties**.
4. Click the **Advanced** tab, and then click **Settings**.

Note: If the *Settings* button is unavailable, the Internet connection firewall is not enabled on this connection, and you do not have to open any ports (because they are all already open).

5. Click **Add**.
6. In the **Description** box, type a friendly name.

   For example, *File Sharing : Port 445*.

7. In the **Name or IP address of the computer hosting this service on your network** box, type 127.0.0.1.

   Note: You can specify the IP address of an internal computer, but the address 127.0.0.1 is typically used.

8. In the **External port** and **Internal port** boxes, type the port number.

   Generally, the same number is used in both cases.
9. Click either **TCP** or **UDP**, and then click **OK**.
10. Repeat steps 1 through 9 for each port that you want to open.

Chapter 2

Working with CobraNet

In This Chapter

Introduction

CobraNet is a reliable and proven technology that enables transport of high quality, real-time digital audio over a standard Ethernet infrastructure.

Note: CobraNet is a technology developed and owned by Cirrus Logic, which sells and/or licenses the technology to third parties. The information contained in this section is subject to change without notice.

CobraNet is an isochronous data delivery system at its core but, Ethernet is not an isochronous data delivery system. Ethernet is a first come, first served, best effort system and will not even guarantee delivery of data. Knowing that, it is easy to see why CobraNet technology represents such an achievement and why certain constraints and operational parameters must be understood in provisioning the Ethernet that CobraNet uses. CobraNet uses Ethernet to perform tasks that Ethernet does not normally do. Therefore, real understanding and proper care are required to ensure consistently good performance.

The primary differences between a CobraNet network and a data network, that an IT professional should note, are as follows:

- Data network traffic is typically *bursty*, whereas CobraNet network traffic is largely consistent.
- CobraNet networks can use far more multicast traffic than normally seen on data networks.
- CobraNet is intolerant of data errors or bandwidth over-subscription that data networks can often tolerate.
- The CobraNet audio protocol itself is strictly layer 2 (Ethernet). It cannot be routed.
- Management functions used by CobraNet are implemented with high-level IP protocols, such as SNMP and TFTP.

Connections

- CobraNet must operate on a full-duplex network. Repeater hubs in the network are forbidden. Collisions cannot be tolerated.
- The connection to a CobraNet device is 100 BASETX copper.
- The switch to which it is connected can communicate with other switches by any standard full duplex Ethernet medium, including copper, fiber, 100 Mbit, gigabit and 10 gigabit.
- CobraNet can be successfully bridged over other transport mediums, such as SONET. As long as the end links are IEEE 802.3 compliant and timing constraints are observed, it will work. Timing constraints are covered in the section *Timing* (on page 11).
- CobraNet will work with dedicated full-duplex wireless links, such as Tsunami.
- Wi-fi, Powerline and Homeplug are alternative Ethernet technologies that operate in half-duplex mode. CobraNet will not work properly with these technologies. However, a PC connected to the CobraNet network through one of these types of links can properly manage the CobraNet devices using SNMP.
- The connection to a CobraNet device must be able to auto-negotiate the connection type.
- If you are using an optical to copper media converter in the link attached to a CobraNet device, make sure it can bridge auto-negotiation. Not all will do this, although absence of this feature is becoming less common.

Notes:

- Low bandwidth, half-duplex links such as these can be overloaded by the large amount of traffic that can exist on a CobraNet network. These links will support SNMP, but may still not work well due to the bandwidth they are exposed to.
- Although CobraNet requires a 100 BASETX full duplex link, never explicitly set switch ports to operate in this mode. This will disable auto-negotiation on the port and the attached CobraNet device will not work.

Traffic

- CobraNet is an IEEE registered protocol that has a protocol number (Ethertype) of 0x8819.
- There are four types of Ethernet frames used by CobraNet that will be seen on the network:
  - *Beat packet* – only sent by a single *Conductor* device.

    Sent 750 times per second (1 1/3 mS being the isochronous cycle time).

    The size of the beat packet depends on the number of CobraNet devices and audio bundles in use on the network.

    It can be as small as approx 200 bytes or can be as large as a full frame

    The beat packet is always multicast

    Identified by 0x00 following the Ethertype field.

    Typically, any CobraNet device on the network can become the Conductor.
  - *Reservation packet* – Sent by all CobraNet devices.

    Sent every 1 ½ to 8 seconds depending on network size.

    Usually small.

    The Reservation packet is always multicast.

    Identified by 0x01 following the Ethertype field.
  - *Audio bundle packet* – Sent by any or all CobraNet devices.

    Can be large or small depending on configuration.

    Each device can send and receive multiple bundle packets every isochronous cycle.

    Can be multicast or unicast depending on configuration.

    Identified by 0x10 following the Ethertype field.
  - *Serial bridge packet* – Sent by any or all CobraNet devices.

    Use is optional; will not be seen in all cases.

    Can be multicast or unicast; typically multicast

    Usually smaller frames.

    Use to bridge low data rate asynchronous (RS-232) traffic.

    Identified by 0x20 following the Ethertype field.
- CobraNet also generates and uses other types of traffic:
  - SNMP is used to monitor and configure the device.
  - TFTP is used to update the device’s firmware.
  - Packet bridge – The CobraNet device can be used as a NIC by an attached host processor.

Some products or implementations will use this feature in which case any type of traffic may be seen sent or received by the CobraNet device.

No more than one bridge packet per device per every 2 isochronous cycles (2 2/3 mS) should be seen sent or received.

- From the above, it can be seen that a CobraNet network will usually contain a finite amount of traffic of known types.
- This traffic can vary widely in makeup between multicast and unicast
- The makeup of the traffic (multicast vs. unicast) will be consistent in an operational installation.
- Total multicast CobraNet traffic on a network can range from less than 1 Mbit/s to all of the traffic that can be supported on the net.
- In a small network, expect to see less than 1 Mbit of multicast beat packets.
- As a general rule, more than four 8 channel multicast bundles on a network will not work. The contractor should be aware of this constraint. If you, as an IT professional, see more than four multicast bundles on the net point this out to the audio contractor and make sure this condition is known and intended. A multicast bundle can be identified by: destination MAC address is multicast, Ethertype = 0x8819, 1st data byte = 0x10.
- In the largest network, expect to see as much as 10 Mbit of multicast beat packets.
- A CobraNet device should not require more than 50 Mbits of bandwidth in each direction. In most cases, half that bandwidth is typical.
- Links between switches can require far more than 50 Mbits of bandwidth. Use gigabit links between switches. The system contractor can relate what the bandwidth requirements of each link will be. Over-provision between switches to ensure good performance and to accommodate future changes.

Notes:

- Do not configure a switch to filter multicast traffic. CobraNet depends on multicast traffic.
- Some switches automatically configure links between two switches as trunking ports. It is common for trunk links to be processed by the CPU in a switch, rather than simply passing traffic through the hardware switch fabric. This can add to the variability of forwarding delay timing and can cause dropouts or loss of clock lock. Always check switch settings to be sure the switch is not using functionality that could add forwarding delay variability. Often, newer switches that use auto configuration, referred to as *smart switches*, can exhibit this problem.

Bandwidth allocation

- CobraNet can theoretically share a network with data traffic.
- Provided that the data traffic is predominately unicast and any links shared by CobraNet and the data traffic are provisioned to ensure that CobraNet will always have adequate bandwidth, then sharing network infrastructure can work.

Note: It is very difficult to predict the types of data traffic that will exist on a network, and it is very difficult to ensure enough available bandwidth on all links given the inconsistent and bursty nature of data traffic. For this reason, segregation of data and CobraNet networks is recommended.

- Networks can be segregated by using separate switches for each network.
- Networks can be segregated by using VLANs.
- CobraNet does not support tagged VLANs. Managed switches with port based VLAN capabilities are used to implement a CobraNet VLAN.
- CobraNet VLANs should be given higher priority on shared links between switches.

Switches

- Although any 802.3 compliant switch should work with CobraNet, some less expensive switches cannot operate at wire speed or have limited queue buffer sizes and can cause problems when a large amount of traffic exists.
- Some less expensive gigabit switches will not operate at 1 Gigabit if any port is in use at 100 Mbit.
- It is best to avoid bargain switches and use good quality switches from reputable manufacturers.
- We strongly encourage the use of managed switches in larger projects for the following reasons:
  - They can be configured to limit broadcast storms or otherwise throttle the data rate on specific ports. This can be a benefit to CobraNet. Do not limit the bandwidth to less than the CobraNet device needs to operate properly.
  - Port mirroring capability is very useful if debugging is necessary.
  - Statistics logging is very useful if debugging is necessary.
  - Use of VLANs can be very useful in large applications.
  - Link aggregation can be very useful to increase bandwidth between switches and to provide a measure of redundancy.
  - STP, RSTP and MSTP can be used to create fault tolerant topologies.
  - QoS can be implemented to ensure that CobraNet has the highest priority.

    CobraNet devices themselves cannot generate or process tagged QOS packets.

    Some protocols, such as VOIP, will also attempt to secure the highest priority. Be sure to consider the types of protocols and priorities that will exist on the network in order to ensure that sufficient bandwidth and priorities are in place for CobraNet.

Timing

CobraNet causes a best effort network technology to perform as an isochronous delivery system. In order for this to work, certain timing constraints must be met.

- Every hop a frame takes through a switch introduces forwarding delay.
- This delay is not always consistent.
- CobraNet cannot tolerate large inconsistencies in forwarding delay.
- Total variation of forwarding delay can worsen with each switch hop.
- The maximum forwarding delay that can be tolerated is no more than 3800 uS (3.8 mS) between the network diameter extremes.
- Whatever this delay is, up to the 3800 uS maximum, it must be relatively consistent between any two CobraNet devices and must not vary by more than –0/+250 uS. Occasional violations of this rule can be tolerated; chronic violations will prevent proper operation of the network.

- It has been empirically determined that the forwarding delay variability in typical 100 BASETX switches limits the number of hops to a maximum of six between any two CobraNet devices.
- Use of gigabit links between switches increases the hop limitation due to a reduction in forwarding delay between switches. However, the forwarding delay can still be variable and this variability, as opposed to the average aggregate delay, is the important factor. Therefore, although more hops can be tolerated when they are gigabit hops, it is still wise to limit the number of hops as much as possible. A properly designed network with a balanced hierarchical layout can contain a huge number of end points while still remaining within the six hop guideline. If your network is using more than this number of hops, it would be useful to reexamine and optimize its layout.
- If the contractor chooses to use lower latency CobraNet settings, the number of hops that can be tolerated will be reduced to two or three hops at 2 2/3 mS latency (or 10-15 with gig links) and one or two at 1 1/3 mS latency. Consult with the system contractor on this issue to determine how CobraNet will be configured.

Note: The above switch hop rules are guidelines only. Different results can be obtained depending on the characteristics of an individual switch and the nature of the traffic on the network.

Wiring

Data networks are more tolerant of data errors than CobraNet networks. Typical layer three and above protocols will retransmit and retry unsuccessful transmissions. CobraNet does not do this. By the time a dropped frame is detected, it is too late to retransmit; that isochronous cycle is gone. For this reason it is important to ensure the integrity of the wiring prior to commissioning. Data error rates that may go unnoticed on a typical data network cannot be tolerated on a CobraNet network.

- Make sure all cables are properly terminated.
- Do not use *kinked* cables. If a cable is kinked during installation, do not straighten it out; use a new cable. The sensitive internal wiring twist which influences noise rejection and maximum data rate has been damaged.
- Do not run cables parallel to AC mains lines.
- Do not run cables close to noise sources, such as motors, fans, compressors, dimmer circuits, A/C lines etc..
- If running longer links or in noisy environments, use optical fiber.
- Use Cat 5e or above for copper 100 BASETX links.
- Use Cat 6 for copper gigabit links when copper must be used. Use fiber instead of copper on gigabit links whenever possible. The way in which data is modulated on gigabit copper makes it more sensitive to outside interference. Therefore, when copper gigabit links must be used, pay particular attention to cable routing and ensure that the cables are not in proximity to any potential noise or interference sources. A data integrity problem on a gigabit link may go unnoticed on a data network but will cause audio dropouts on a CobraNet network.
- If possible, perform bit error rate tests on each link and correct problems before commissioning.
- Check switch statistics for indications of errors and dropped or malformed frames. Find the root cause and correct it before commissioning.

- Do not exceed the maximum recommended run length of the media in use, i.e. no more than 100 meters for copper Ethernet cables. Fiber run lengths can vary depending on cable and switch manufacturer. Typically lengths of no more than 2 km are recommended for 100 megabit multimode fiber, 600 meters for gigabit and 300 meters for 10 gigabit. Single mode fiber supports much longer runs but is also more expensive and seldom used in LAN applications. Consult the documentation for the particular equipment and wiring used in order to ensure maximum lengths are not exceeded.

Note: A large CobraNet network can sometimes be complex to commission. Make sure the systems contractor only has to focus on his own tasks and does not have data integrity issues to debug as well. Ensure that the network is operating as required before handing it over to the contractor.

Supported CobraNet firmware

Product	**Variant**	**Firmware version**
NION	CM-1 rev F	2.9.16.3 (nion_2_9_16_3.bin)
	CM-1 rev J	2.21.17.3 (nionp311_2_21_17_3.bin)
CAB 4n	CM-1 rev F	2.9.11.2 (cab4n_2_9_11_2.bin)
	CM-1 rev J	2.21.16.11 (cab4np311_2_21_16_11.bin)
	CM-2	2.11.6.4 (cab4n2_2_11_6_4.bin)
CAB8n	CAB8nc	Alpha 0.2 CobraNet version 2.11.6 CS496112 (cab8nLJ_2_11_6_4.bin)
nWall	Silicon Series	2.11.6.4 (cs18101_2_11_6_4.bin)
Legacy CABs	CAB 8i	2.9.12 (cab8i_2_9_12.bin)
	CAB 8o	2.9.12 (cab8o_2_9_12.bin)
	CAB 16d	2.9.12 (cab16d_2_9_12.bin)
	CAB 16i	2.9.12 (cab16i_2_9_12.bin)
	CAB 16o	2.9.12 (cab16o_2_9_12.bin)
	X-Bridge	2.9.12 (xbridge_2_9_12.bin)
MainFrame	DSP-CN card	2.9.12 (cndsp_2_9_12.bin)
	DSP-CN2 card	2.9.12 (dspcn2_2_9_12.bin)

Chapter 3

Using XDAB clusters with VLANs and CobraNet

In This Chapter

Introduction

Use of NIONs in an XDAB cluster, particularly when also using CobraNet and VLANs, creates specific considerations and rules that must be observed in order to ensure proper operation of the system. This chapter is intended to provide awareness of the technical issues that must be considered when using XDAB clusters and VLANs with CobraNet. A basic knowledge of CobraNet, NIONs and VLANs is assumed.

Note: XDAB is available on NION n3 and N6 models, but not nX or nE models.

Important concepts

XDAB cluster

NIONs connected together via XDAB are referred to as an XDAB cluster.

There is one XDAB master that provides the audio clock to all other devices in the cluster. The other devices in the cluster are XDAB slaves.

Audio clock domain

All CobraNet devices on the same network or VLAN segment must operate within the same audio clock domain. A system wide isochronous audio clock is automatically generated. A NION or CAB will always receive its audio clock from CobraNet.

However, if NIONs are operating within an XDAB cluster, the behavior is different:

- In the XDAB master, the CobraNet clock can be taken from the CobraNet network as a CobraNet Performer or the XDAB clock can be supplied as the CobraNet Conductor. Normal CobraNet clocking concepts apply.
- In XDAB slaves, the CobraNet clock will always be taken from XDAB and will not be taken from the CobraNet network audio clock directly. The clock will be taken indirectly from CobraNet via the clock generated by the XDAB master.

Logical separation of the network

Use of VLANs creates a logical separation of the network that causes the VLAN segments to behave as if they are physically separate networks. Use of the term VLAN also applies to physically separate networks.

Each VLAN segment must therefore have its own CobraNet Conductor.

Multiple VLANs

Audio can be exchanged between different VLANs through the use of devices that have a network interface on each VLAN. This can be accomplished by:

- exchanging analog audio between devices. Devices connected using analog I/O do not need to be concerned with audio clocking issues between them.

or

- exchanging digital audio between devices. In this case, the audio clocks of the devices must be synchronous *or* the use of sample rate converters on the digital audio inputs is required.

Tip: The XDAB digital audio bus is the most convenient way to exchange digital audio between NIONs.

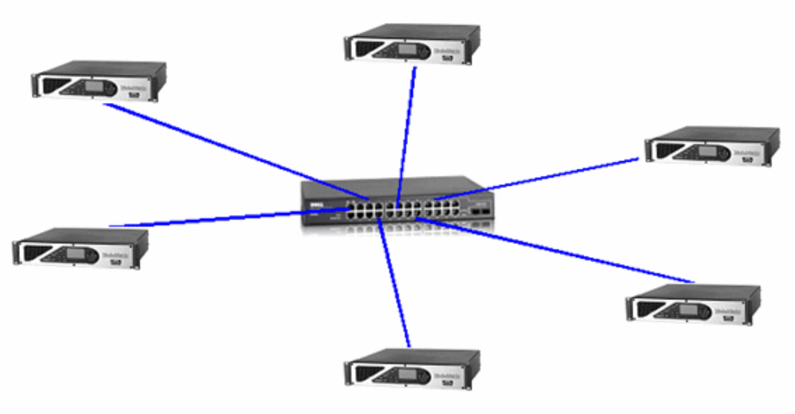
NIONs on CobraNet

Notes:

- Processing on a NION will pause during project deployment. Therefore, a NION that is a Conductor will stop being the Conductor for a time. The network will then automatically transition to a new Conductor. Conductor transitions will cause momentary audio dropouts. It may therefore be desirable to designate a non-NION device to be the CobraNet Conductor.
- Additionally, if using XDAB, clock disruption caused by a change of Conductor may often cause the NION cluster to re-sync (re-arbitrate) the XDAB clock and will result in a dropout of several seconds.

Use cases

Scenario 1 - Basic network

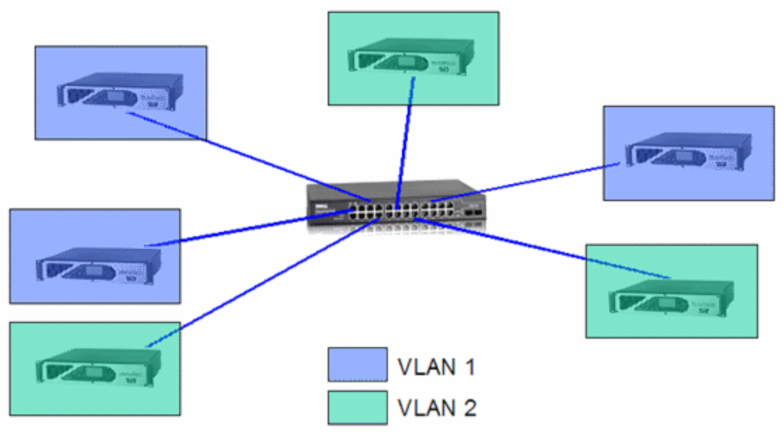


In this scenario, there are:

- no XDAB interconnections between NIONs.
- no VLANs defined.
- no outboard audio connections, either analog or digital, between NIONs.

There is only one audio clock domain in this scenario established by CobraNet and no special Conductor, topology or XDAB usage considerations apply.

Scenario 2 - Network using VLAN

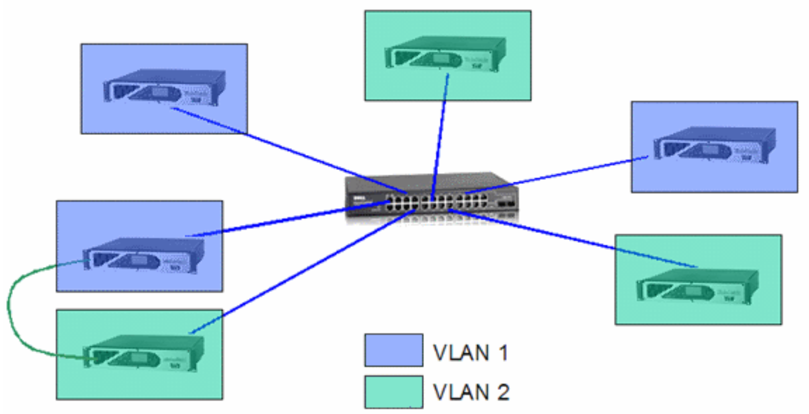


In this scenario, port based VLANs have been configured within a managed switch:

- There will be no audio passed, either externally or via , between devices residing on different VLANs.
- Audio is only exchanged via between NIONs that reside on the same VLAN.
- One device on each VLAN must be a Conductor for that VLAN, i.e. each VLAN has its own Conductor.

It is not important, logically, which devices are chosen to be Conductors. Consideration of Conductor location will only be determined when necessary, by standard network topology considerations that would apply to any network.

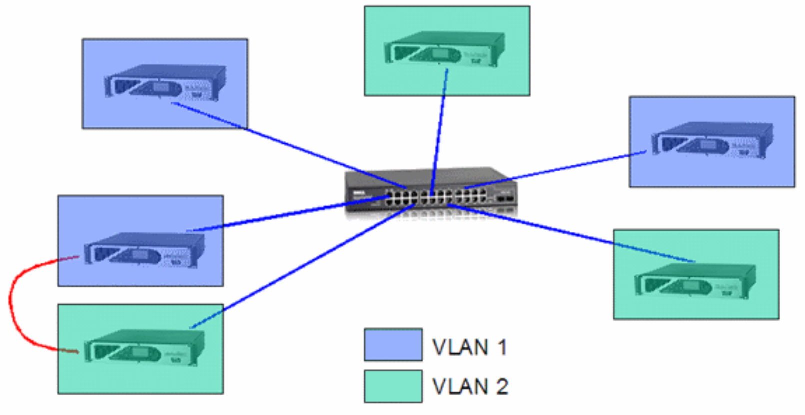
Scenario 3 - Network with VLAN and analog interconnects



In this scenario, VLANs are configured using the port based VLAN capability of a managed switch.

- Audio is bridged between the two VLANs using analog interconnects.
- The same rules for CobraNet Conductors would apply as in the previous scenario.
- The analog interconnect creates no digital audio clock domain issues.

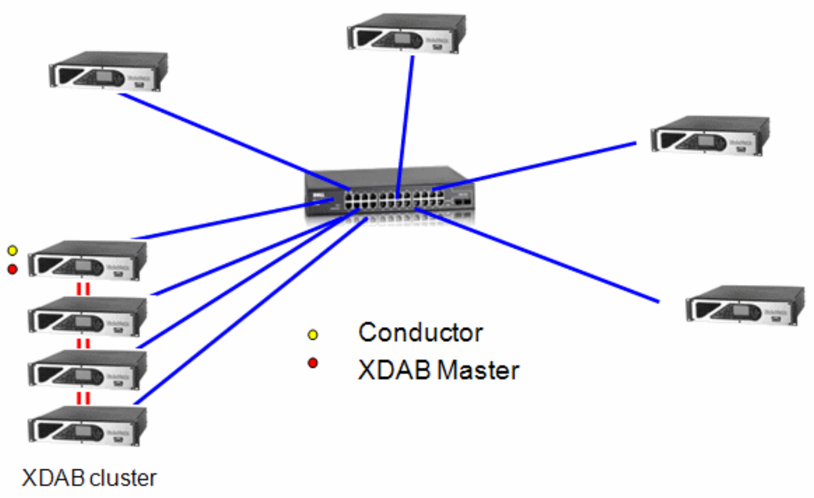
Scenario 4 - Network with VLAN and digital interconnects



This scenario is similar to the *previous scenario* (on page 18), but substitutes digital interconnects, such as AES/EBU or SPDI/F, for analog interconnects.

- NION digital interface cards contain built-in sample rate converters (SRCs), which isolate audio clock domains from each other and allow interchange of digital audio data regardless of which clock domain the transmitting and sending devices are in.
- VLAN 1 and VLAN 2 each have their own Conductor, so are in different audio clock domains.
- The SRC built into the digital interface card will allow exchange of digital audio between the NIONs in the two clock domains.
- Bypassing the SRC, which is possible, will cause errors on the AES/EBU interface.

Scenario 5 - Network with an XDAB cluster (CobraNet)



In this scenario, digital audio is exchanged between NIONs through XDAB.

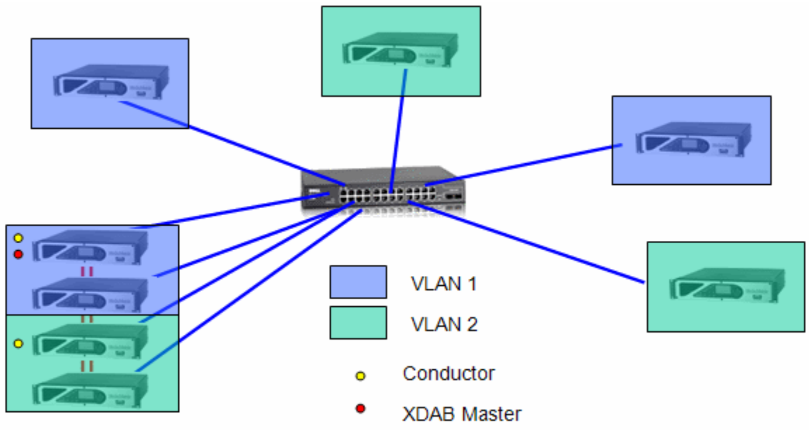
- The XDAB master can be any device within the cluster.
- The CobraNet Conductor can be any device outside the cluster.
- Remember that all XDAB slaves and their CobraNet interfaces take their clocks from XDAB.

- An XDAB master that gets its clock as a CobraNet performer that is synched to a Conductor that is in turn an XDAB slave would create an unstable clock resolution loop. XDAB would attempt to sync with CobraNet that would in turn be trying to sync with XDAB.
- The XDAB master and CobraNet Conductor will both be in the same NION automatically when default settings are used. If default settings are changed, then be sure to set the XDAB priority and CobraNet Conductor priority to ensure that a single NION is both the XDAB master and CobraNet Conductor.

Notes:

- If the Conductor is placed within the cluster, then it must also be in the same NION as the XDAB master. If you increase the Conductor priority for one of the NIONs, you *must* also increase its XDAB priority to ensure that the Conductor and XDAB master will stay in the same NION.
- If a Conductor for a CobraNet network is placed within an XDAB cluster, the NION containing the Conductor must also be the XDAB master.

Scenario 6 - Network with VLAN and XDAB



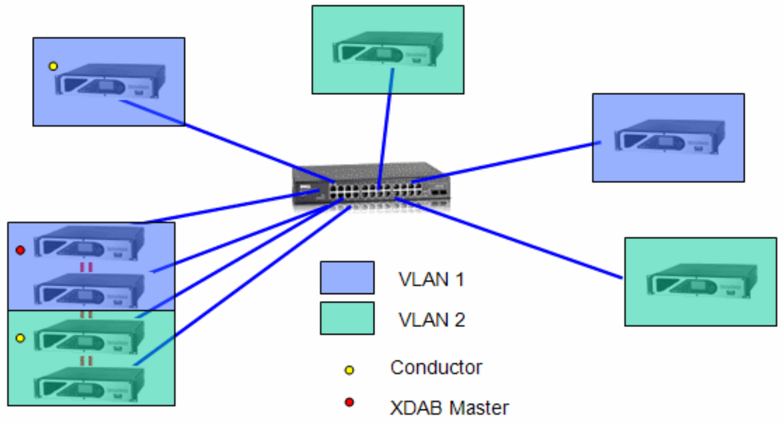
In this scenario, the network is divided into VLANs and an XDAB cluster is used. Two VLANs are shown; more are possible.

- XDAB is used to pass digital audio between NIONs within a cluster and therefore between VLANs.
- VLANs logically become one of two types in this scenario:
  - A master VLAN, i.e. the VLAN in which the XDAB master resides.
  - A slave VLAN, i.e. all other VLANs in the cluster.
- The Conductor on the one master VLAN must be either:
  - completely outside the XDAB cluster

    or
  - must also be the XDAB master.
- The same caveats regarding Conductor location as described in the *previous scenario* (on page 19) must be observed. But it is also important to properly locate the CobraNet Conductors for the slave VLAN (VLAN 2) to be sure that a clocking conflict is not created between XDAB and VLAN 2’s CobraNet clock.

- Regardless of whether the VLAN 1 Conductor is inside or outside of the cluster, all NIONS in the cluster that are in VLAN 2 will be getting their clock from XDAB and cannot receive their clock from an outside Conductor. This would create a clocking conflict.
- Therefore, the Conductor for VLAN 2 must be located within the XDAB cluster, as shown.

Scenario 7 - Network with VLAN and XDAB

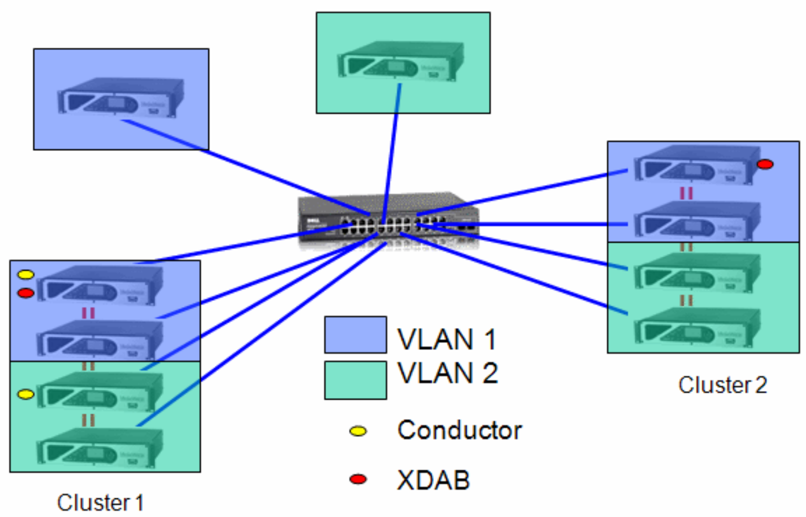


This scenario is a variant of the *previous scenario* (on page 20).

- The Conductor for VLAN1 is outside the XDAB cluster. This will still work.
- The CobraNet interface in the XDAB master will sync to the Conductor outside the cluster. That clock will become the XDAB master clock. XDAB and VLAN 1 will be in sync.

  However, the Conductor for VLAN 2 must still remain within the cluster because all XDAB slaves in a cluster will receive their clock from XDAB and not from CobraNet.
- Placement of VLAN 2's Conductor outside the cluster will cause the XDAB clock and externally sourced VLAN 2 CobraNet clock to be in conflict.

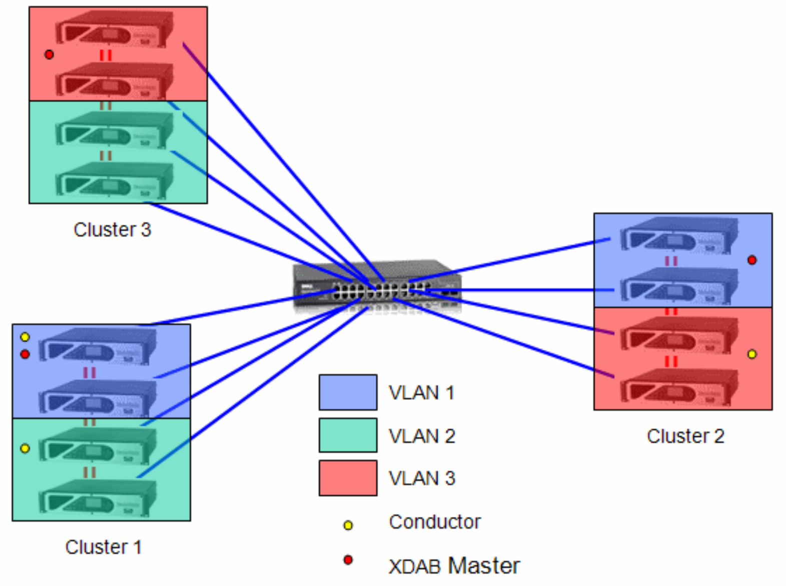
Scenario 8 - Network with VLAN and two XDAB clusters



This scenario is a variant of the *previous scenario* (on page 21), but contains more than one XDAB cluster.

- The same rules apply as in the previous scenario.
- Again, the Conductor for VLAN 2 must be within the XDAB cluster.
- It does not matter which cluster the Conductors are in. In this case, the Conductors are show in cluster 1.
- In this example, it does not matter which device in cluster 2 is the XDAB master. The XDAB master will receive its audio clock from a CobraNet Conductor in either VLAN 2 or VLAN 1, both of which are in sync with each other.
- The clock received by any device in cluster 2 via CobraNet will be the same because the Conductors for both VLANs are in cluster 1 and are synched to the same clock.

Scenario 9 - Network with VLAN and three XDAB clusters

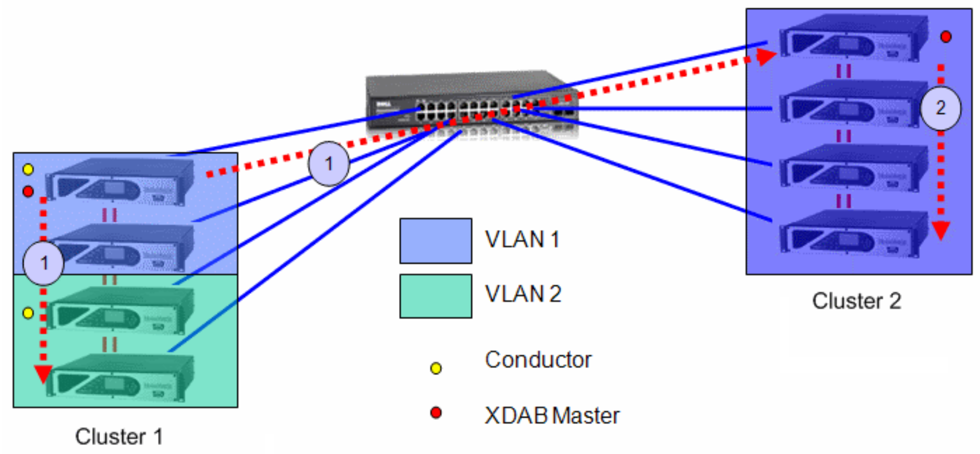


In this scenario, there are three VLANs, three XDAB clusters and no cluster contains all three VLANs.

- In cluster 1, VLAN 1 contains the XDAB master.
- In cluster 1, VLAN 2 receives its clock from XDAB and is therefore in sync with VLAN 1.
- In cluster 2, VLAN 1 is the XDAB master and receives its clock from the VLAN 1 Conductor in cluster 1.
- In cluster 2, VLAN 3 receives its clock from XDAB. This clock is derived from the Conductor of VLAN 1.
- In cluster 2, one of the devices in VLAN 3 is the Conductor for VLAN 3.
- In cluster 3, VLAN 3 is the XDAB master and receives its clock from the Conductor in VLAN 3 in cluster 2.
- In cluster 3, VLAN 2 is receiving its clock from the XDAB master in VLAN 3.
- All Conductors in this topology are ultimately deriving their clocks from the Conductor and XDAB master in VLAN 1 of cluster 1. So all clocks in this network in all three VLANs will be in sync. No clock conflicts will exist.

Further examples

Worked example 1 - follow the clock

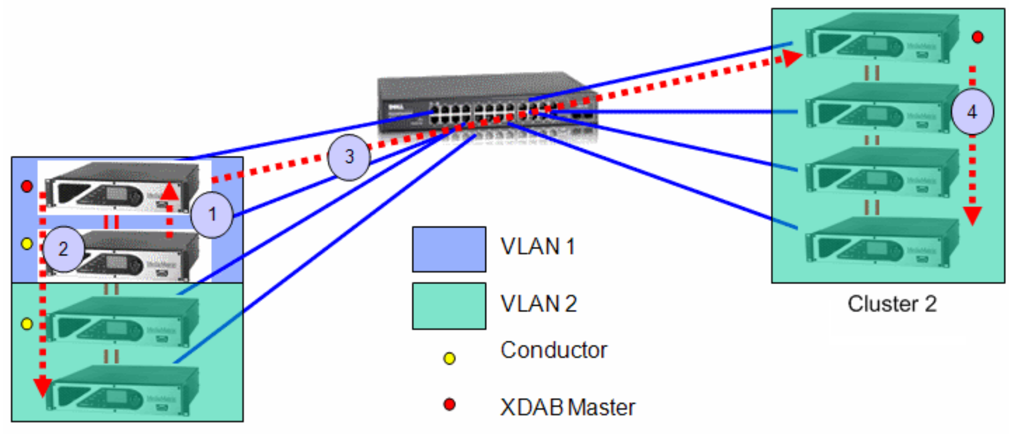


- An XDAB master NION will always receive the audio clock from its CobraNet module, regardless of whether that module is a Conductor or a performer.
- If the CobraNet clock source is external to the cluster (i.e. the XDAB master is a performer and the Conductor is external to the cluster), it will still work fine.
- If the clock source is internal to the cluster (i.e. the CobraNet Conductor is within the VLAN within the cluster), then the XDAB master and the CobraNet Conductor *must* be the same.

Notes:

- In the example above, the clock source is the CobraNet Conductor (clock path 1). This Conductor NION must also be the XDAB master. Clock 1 will be transmitted by XDAB to the other devices in the cluster and also to the other cluster on the network via CobraNet.
- In Cluster 2, the XDAB master is a performer.

Worked example 2 - a bad configuration



- The Conductor for VLAN 1 is the second device in the VLAN 1 segment within XDAB Cluster 1. It is therefore the clock source for VLAN 1 (clock path 1).
- The XDAB master in Cluster 1 is therefore a CobraNet performer in VLAN 1.
- The audio clock will originate in the Conductor from which the XDAB master (a performer) will get its clock via CobraNet.
- The performer, XDAB master, will then supply its clock to the XDAB chain (clock path 2) from which the Conductor will get its clock.
- A *clock loop* exists in this example.
- The XDAB master is relying on the CobraNet Conductor for its clock source, delivered to it via CobraNet., but the CobraNet Conductor is relying on the XDAB master for its clock source delivered to it via XDAB.
- Both devices consider the other one to be their clock source and so neither can provide a stable clock to the other.
- Clock Path 1 is a CobraNet clock distributed on the network and is an unstable clock for reasons outlined above. Therefore, the audio clock in cluster 2, which is received on clock path 1 and propagated via XDAB to the other devices in the cluster, will also be unstable. No device in Cluster 1 or Cluster 2 will have a stable audio clock.

Note: It may be possible for the two clocks (XDAB master and Conductor in cluster 1) to become stable and synchronous. But this will be a time consuming matter of chance, rather than a deterministic certainty, as the XDAB chain attempts to arbitrate a master. In the absence of any beneficial timing coincidences at the beginning of a sync attempt, the clocks would never sync up.

MediaMatrix®
A Division of Peavey Electronics Corp.

5022 Hartley Peavey Drive, Meridian Mississippi, 39305, USA

Phone: 866.662.8750

http://www.peaveycommercialaudio.com/products.cfm/mm/

80307498