Ashly CobraNet Networking Basics

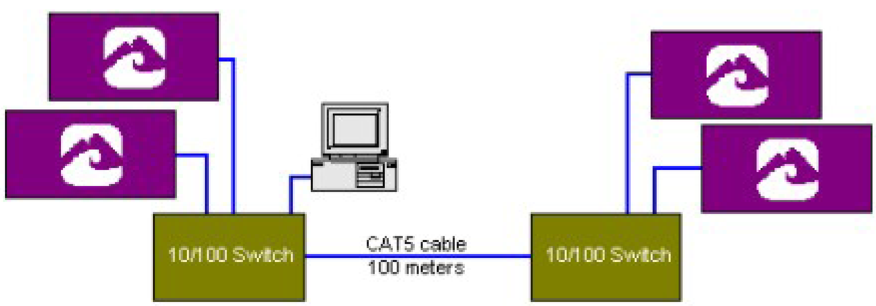
Can I Use the Same Network for my CobraNet and Ethernet Connections?

It is generally a good idea to have two separate Ethernet networks for control and CobraNet audio. The issue is this: CobraNet audio is uncompressed raw samples that need to be transmitted(and received) at a constant rate. Control traffic is usually random and "bursty". When you have a single Ethernet network, all of that control and audio data has to flow through the same pipe. So if a flurry of control packets comes along and is enough to delay transmission or reception of audio packets, you're going to get glitches in the audio. These typically will be heard as pops or clicks. This is most noticeable if you have a large number of channels on the network.

Usually, these glitches are rare. Control packets tend to be short and because of this, they can slide in and around the audio packets without any problem. But even short control packets can overwhelm audio packets if there are a lot of them.

Switches (even the dumbest ones) are smart enough to direct traffic to the proper port. So control packets destined for a computer won't be seen by the CobraNet interface. Likewise, the switch prevents audio packets between CobraNet interfaces from being seen by the computer. The exception is broadcast (or multicast) traffic. When you send broadcast (or multicast) traffic from either the computer or CobraNet interface, that packet is sent to all ports on the switch. This is why it is strongly recommended that all traffic is unicast. That means on the control side, making sure that the IP addresses being used are specific (not things like "255.255.255.255" or "192.168.1.255") and that on the CobraNet side, you're using bundle numbers between 1 and 255.

The problem is that you can't always control this. Take this picture of a CobraNet network (this comes from their own site):

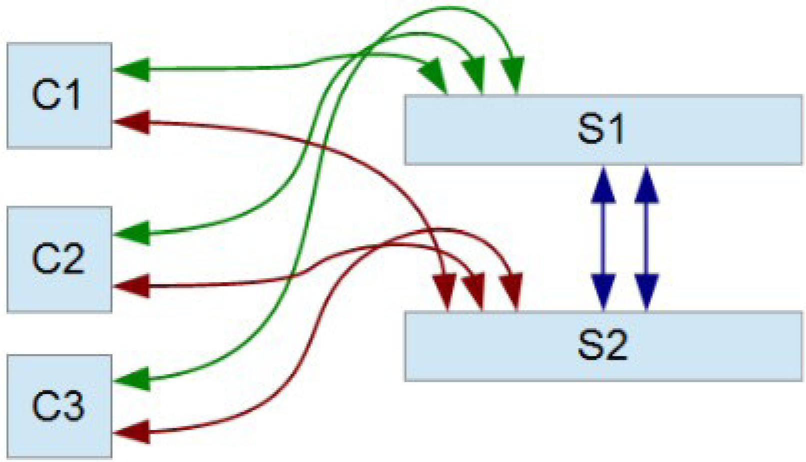


You'll note that in this network, control (from the computer) and audio flow use the same network. That's fine, but Windows computers are chatty, and they by default will send random broadcast traffic (mostly announcing themselves on the network). If you don't know how to control this, it can potentially glitch the audio.

Smarter (and more expensive) switches can deal with this another way. Using features like QoS (Quality of Service) and VLANs (virtual LANs) you can handle broadcast (or multicast) traffic without having two separate networks. But this requires some skill, deeper understanding of networking, and money for the smarter switches. So generally, it's easier to just get two dumb switches and keep the networks separated.

Primary and Secondary Connections

The CobraNet interfaces have primary and secondary jacks which are required in fault-tolerant systems. The simple notion is that if the primary fails, the secondary takes over. One possible way to configure such a redundant network is to connect the primary and secondary jacks to the same switch. This works, but only makes the connection to the local switch fault tolerant. More typically, people would set up something like this:



In this configuration, three CobraNet interfaces are connected to two separate switches. The primary jacks (green) connect to one switch, the secondary jacks (red) connect to the other switch. Then, both switches are connected to each other. This handles the case of a primary connection failing on a CobraNet node, whereby the secondary connection automatically takes over upon failure of the primary data stream. It also handles the case of either switch failing.

Note that this diagram shows the CobraNet interfaces all close to each other. If one or more CobraNet interfaces are separated by a large distance, then cable run length limits and other practical concerns may lead to a different topology.

Also note that this diagram shows redundant connections (blue) between the network switches. This is so that if one link between the switches fails, the other takes over, a fundamental requirement for redundant CobraNet systems. To have two (or more) links between switches, all switches must support and be properly configured for Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP), as they prevent the redundant links between switches from becoming loops.

ASHLY AUDIO INC. 847 Holt Road Webster, NY 14580-9103, USA
Phone: (585) 872-0010 Fax: (585) 872-0739 Toll Free (800) 828-6308 www.ashly.com