

Common Problems and Solutions

Dropouts or errors due to no auto-negotiation

Symptoms: Audio dropouts and/or transmit error indication.

Cause: If auto-negotiation is disabled, switch ports must be configured manually *at both ends*. CobraNet™ devices do not provide a means for manual configuration. CobraNet™ devices use auto-negotiation to determine whether they are attached to a switched or repeater network. When auto-negotiation is disabled (and the switch port is configured manually) a CobraNet™ device will assume it is connected to a repeater hub and establish a half-duplex connection. Even if the switch port is configured for half-duplex operation, thinking it is connected to a repeater network, the CobraNet™ device will have activated its collision avoidance mechanism. This mode of operation is inappropriate on a switched network and may result in intermittent audio transmission problems.

Solution: Configure all switch ports to auto-negotiate. This is the factory default setting for almost all managed and unmanaged switches.

Dropouts due to 100BASE-FX connections improperly configured on switches

Symptoms: Audio dropouts between switches. Poor network performance.

Cause: Auto-negotiation is only supported on copper Ethernet variants (10BASE-T, 100BASE-TX, 1000BASE-T). Link operating mode for fiber variants (10BASE-FL, 100BASE-FX, 1000BASE-SX, 1000BASE-LX) must be configured manually. Mismatched or inappropriate operating modes results in sub-optimal performance and/or packet loss.

Solution: Configure all fiber links between switches for full-duplex operation. Default fiber port configuration (for historical reasons) is typically half-duplex. A configuration step needs to be performed on fiber links. These steps are enumerated in our published setup procedures for HP and 3Com switches.

Improper use of uplink port on LinkSys hubs

Symptoms: Collisions and/or "partition" indication on hub ports.

Cause: Some LinkSys hubs share the connection on the *Uplink Port* with the port next to it. Connecting devices to both of these jacks results in two Ethernet devices connected to a single Ethernet port. This is an illegal wiring configuration and generally results in the symptoms indicated above.

Solution: Follow the instructions or the documentation that came with your hub on how to enable or use the *Uplink Port* on your hub or switch.

Dropouts due to too much multicast traffic on a switched network

Symptoms: Audio dropouts. Possible transmit error condition on half-duplex CobraNet™ devices (QSC RAVEs). Poor network performance for non-audio applications.

Cause: Audio can be transmitted with either unicast or multicast addressing using the unicast or multicast bundle assignments respectively. Multicast addressed data is delivered to all points on the network. This traffic can overload network connections. Therefore the quantity of multicast audio transmissions on a network must be controlled.

Solution: Follow the guidelines given in the Bundle Assignments in CobraNet™ Systems Application Note.

Dropouts or faults due to a loop in the network

Symptoms: Severe audio dropouts, transmit, receive and fault indications on CobraNet™ devices. Lockup of computers and other peripherals connected to the network. Poor to non-existent network performance.

Cause: A broadcast storm is created when an Ethernet network is wired in a loop topology - a single packet is forwarded endlessly around the loop in the network. This situation is analogous to audio feedback. The network is flooded with the recirculating broadcast packets and is hard pressed to deliver any useful data.

Solution: Rewire the network as to remove any loop conditions. Enable spanning tree protocol, link aggregation or meshing features. Note that "broadcast storm control" features on many switches can limit the damage and extent of a storm, but these features do not address the root source of the storm.

Data errors on network due to malfunctioning network equipment or cabling

Symptoms: Audio dropouts. CRC (Cyclical Redundancy Check) or FCS (Frame Check Sequence) errors reported by switches and/or CobraNet™ equipment.

Discussion: Ethernet packets contain a mathematical integrity check called a CRC code. The CRC code allows detection of any corruption of packet data during transit across the network. If corruption is detected, the packet is dropped. Most managed network equipment maintains counters indicating the number of these errors detected during operation. The counters are accessible via SNMP on any SNMP managed networked device as ifInErrors (1.3.6.1.2.1.2.2.1.14.n where n is the port number). The counters are also available via the console or Web interface on managed switches.

Cause: Packet corruption indicates malfunctioning network equipment, malfunctioning CobraNet™ equipment or problems with cabling. The Ethernet interface is responsible for driving a cable and decoding the signals coming over the cable. Marginal performance from the interface at either end of the cabling, marginal performance from the cabling itself or external electrical interference can potentially produce data corruption.

Solution: Marginal cabling can usually be identified through use of a CAT5 cable tester. Common cabling problems include wrong pairing and wrong connectors. Problems at the Ethernet interface must be isolated by swapping equipment. If a particular device is frequently reporting problems try swapping out the device, switching its connection to a different switch or hub port or swapping out the switch or hub in order to isolate the problem. Remember that the device reporting the problem is not necessarily the source of the problem.

Dropouts or faults due to legacy CobraNet™ firmware on switched networks

Symptoms: Audio dropouts, error indications on CobraNet™ devices.

Cause: CobraNet™ was first introduced for use on repeater networks. CobraNet™ now supports operation on switched networks. Very early versions of CobraNet™ firmware did not support switched networks. Later firmware versions supported simple switched networks but had difficulty with larger installations.

Solution: Contact the equipment manufacturer for updated firmware. Normally the new firmware update can be achieved centrally through the network with the CobraNet™ Discovery application (Disco).

Receive or transmit errors due to wrong pairing in CAT5 cable

Symptoms: No link indication or intermittent link indication at hub and/or CobraNet™ device. Receive and/or transmit error indication on CobraNet™ device. Audio distortion.

Cause: An Ethernet connection over CAT5 utilizes two transformer balanced connections: one for transmit and one for receive for a total of 4 electrical connections. The two electrical connections comprising a balanced pair must be carried on a pair of conductors twisted together. The twisted pair acts as a transmission line for the high frequency Ethernet signals. Attempting to transmit these signals over two independent (untwisted) conductors results in excessive signal attenuation, cross-talk and susceptibility to electromagnetic interference.

Solution: Follow proper cabling guidelines when terminating CAT5 cable.

No or intermittent link due to wrong type of RJ45 connector

Symptoms: No link indication or intermittent link indication at hub and/or CobraNet™ device. Loss of network connectivity when cables are flexed.

Cause: There are different types of RJ45 connectors for different types of cable. Use of the wrong connector results in intermittent or high impedance connections.

Solution: Connectors appropriate for the cable type must be used to assure reliable connections. This issue is discussed in detail on the Network Cabling page.

Dropouts due to greater than 64 channels on a *repeater* network

Symptoms: Audio dropouts. Bundle transmitter fails to transmit.

Cause: A repeater network provides 100Mbit of bandwidth network wide. This bandwidth corresponds to 64 CobraNet™ audio channels at 20 bit resolution. Attempting to carry more than 64 channels overloads the network.

Solution: Use of repeater hubs is not recommended. Use switches instead of repeater hubs OR insure that no more than 64 channels are carried on a repeater network.

Dropouts due to network built of hubs and switches

Symptoms: Audio dropouts. Constant collision indication on repeater hub. In many circumstances no problems are encountered until specific audio routing scenarios are configured for the network.

Cause: CobraNet™ has two operating modes: one for repeater networks and one for switched networks. Different strategies are used on the different types of networks to insure reliable delivery of audio data. A hybrid network built of switches *and* repeater hubs is not a permissible configuration for a CobraNet™ network because neither the switched network nor repeater network strategies are effective at insuring reliable delivery of data on such a network.

Solution: Use of repeater hubs is not recommended. CobraNet™ should be deployed on a switched network. A switched network should have no repeater hubs. If repeaters are used, a repeater network should have no switches. A repeater hub is permissible on a switched network only in the case where no CobraNet™ devices are connected to the hub.

Dropouts due to unregulated traffic on a *repeater* network

Symptoms: Audio dropouts. Transmit and receive error indication on CobraNet™ devices.

Cause: If CobraNet™ is to be used on a repeater network it must be a dedicated repeater network. Traffic from PCs and other non-CobraNet™ devices interferes with CobraNet™'s collision avoidance mechanisms resulting in audio dropouts.

Solution: Use of repeater hubs is not recommended. Use switches instead of repeater hubs OR remove non-CobraNet™ devices from a CobraNet™ repeater network.