LogiCue
NuDelta Digital

Managed Switch Configuration for LogiCue NET

Managed switches have many settings that, if not configured correctly, could cause your LogiCue NET System to not function properly. Here is a list of settings that should be looked at when configuring a managed switch for use with a LogiCue NET System.

CRITICAL SETTINGS (Check These First)

1. IGMP Snooping Configuration

Symptoms if misconfigured:

- Cue lights loses connection every 5-10 minutes (typically at exact intervals matching membership timeout)
- Works initially but stops receiving multicast traffic
- Works fine on unmanaged switches

Settings to check:

- **IGMP Snooping Admin Mode (Global)**: Should be **Enabled**
    - If disabled, equipment may not connect at all
- **IGMP Snooping per VLAN**: Should be **Enabled** on the VLAN your equipment uses
- **CRITICAL FIX: Unknown Multicast Forwarding** or **Multicast Router Interface Mode**:
    - Should be **Disabled** (allow unknown multicast forwarding) OR set to **Forward Unknown Multicast**
    - **This is the most common cause of periodic timeouts (every 5-10 minutes)**
    - May be called:
        - "Exclude Mrouter Interface Mode" → Set to **Disabled**
        - "Block Unknown Multicast" → Set to **Disabled**
        - "Drop Unknown Multicast" → Set to **Disabled** or **Forward**
        - "Unknown Multicast Behavior" → Set to **Flood** or **Forward**
    - When enabled, the switch drops multicast streams that don't have active IGMP memberships

    - **Extending the membership timeout does NOT fix this - you must allow unknown multicast forwarding**
- **Multicast VLAN**: Configure the VLAN as a multicast VLAN if your switch supports this designation
    - This may automatically configure proper multicast forwarding behavior
- **IGMP Membership Interval/Timeout**: Default is often 260-600 seconds
    - This setting alone will NOT prevent disconnects if unknown multicast is blocked
    - Only matters if equipment can be configured to send IGMP Join messages
- **Multicast Router Port**: May need to designate an uplink port as a static multicast router port

---

2. Port Administrative Status

Symptom if misconfigured: Port doesn't work at all, no link light

Setting to check:

- **Admin Mode** or **Port Status**: Must be **Enabled** or **Up**
- Check all ports where equipment is connected

---

3. VLAN Membership

Symptom if misconfigured: Equipment cannot communicate with other devices

Settings to check:

- All equipment ports must be in the **same VLAN** (typically VLAN 1 or default VLAN)
- Port VLAN mode should be:
    - **Untagged** for cue lights and controller
    - **Tagged/Trunk** only for switch-to-switch connections
- Verify ports are not **excluded** from the VLAN

COMMON ISSUES

4. Storm Control (Broadcast/Multicast Rate Limiting)

Symptom if misconfigured: Intermittent connectivity, especially with discovery protocols

Settings to check:

- **Broadcast Storm Control**: Should be **Disabled** or set to high threshold
    - If enabled with low threshold, can block DHCP, ARP, and device discovery
- **Multicast Storm Control**: Should be **Disabled**
    - If enabled, can rate-limit or block multicast streams
- **Unknown Unicast Storm Control**: Should be **Disabled**

Typical thresholds if Storm Control must be enabled:

- Set to 10-20% of bandwidth or >5000 packets per second
- Check per-port storm control settings, not just global

---

5. Spanning Tree Protocol (STP)

Symptom if misconfigured: 30-50 second delay before port becomes active or cue lights do not connect at all. If possible, turn off STP globally. If it is necessary for other equipment on the switch, leave it on globally and turn it off at each port.

Settings to check:

- **STP Mode on Ports**: Should be disabled for the ports that have cue lights or a controller.
    - If enabled, port goes through listening/learning states (causes delay)
- **PortFast** or **Edge Port Mode**: Should be **Enabled** on ports
    - Bypasses STP delays for end-device ports
    - Do NOT enable on switch-to-switch connections
- **BPDU Guard**: If enabled, ensure end devices don't send spanning tree packets

---

6. Port Speed and Duplex

Symptom if misconfigured: Intermittent connectivity, slow performance, packet loss

Settings to check:

- **Auto-Negotiation**: Should be **Enabled** on switch
    - If disabled on one side, may cause mismatch
- **Speed/Duplex**: If auto-negotiation fails:
    - Some Gigabit switch ports may need to be configured to advertise 10/100
    - Check that port is not restricted to "1000 Mbps only"
    - **Never mix auto-negotiation on one side with forced settings on the other**

ADDITIONAL CHECKS

7. Link Aggregation (LACP)

Setting to check:

- **LACP Mode**: Should be **Disabled** on access ports (ports connecting to controller and cue lights)
- Only enable on switch-to-switch trunks if intentionally creating a LAG/port channel

---

8. MAC Address Aging Time

Symptom if misconfigured: Periodic connectivity loss (very rare)

Setting to check:

- **MAC Address Aging Interval**: Default is typically 300-3600 seconds
- If set too low (< 300 seconds), can cause MAC table to flush active devices

---

9. Energy Efficient Ethernet (EEE) / Green Ethernet

Symptom if misconfigured: Periodic signal loss at cue lights, usually at regular intervals

Setting to check:

- **EEE/Green Ethernet**: Should be **Disabled** on ports with real-time equipment
- If enabled, ports enter low-power mode during "idle" periods
- May cause brief link interruptions

---

10. Multicast Filtering / IGMP Filtering

Settings to check:

- **IGMP Filter Profiles**: Should not be applied to ports
- **Maximum Multicast Groups per Port**: Ensure limit is not too restrictive
- **Multicast VLAN Registration (MVR)**: Should be disabled unless specifically configured

---

QUICK DIAGNOSTIC STEPS

When Equipment Won't Connect:

1. Check **Port Admin Status** - is port enabled?
2. Check **VLAN Membership** - are all devices in same VLAN?
3. Check **Speed/Duplex** - any negotiation errors?
4. Temporarily **disable IGMP Snooping** - does equipment work?

When Equipment Connects Then Disconnects After ~10 Minutes:

1. **PRIMARY FIX:** Set **Unknown Multicast Forwarding** to **Allow/Forward** (disable blocking/exclusion)
2. Designate VLAN as a **Multicast VLAN** if that option exists
3. Disable **Exclude Mrouter Interface Mode** or similar blocking setting
4. Check **Multicast Storm Control** - should be disabled
5. As last resort, enable IGMP membership reports in equipment if possible

When Equipment Has Intermittent Issues:

1. Check **Storm Control** settings - disable or increase thresholds
2. Check **STP** - enable PortFast/Edge Port on access ports
3. Check **EEE** - disable on critical ports
4. Review switch logs for port errors or security events

RECOMMENDED "SAFE" CONFIGURATION

For ports connecting to LogiCue NET equipment:

Setting	Recommended Value
Port Admin Mode	Enabled
VLAN Membership	Untagged member of equipment VLAN
Multicast VLAN	Enable if option exists
IGMP Snooping (Global)	Enabled
IGMP Snooping (VLAN)	Enabled
Unknown Multicast Forwarding	**Allow/Forward/Flood**
Exclude/Block Mrouter Mode	**Disabled**
Storm Control	Disabled
Spanning Tree PortFast	Enabled
Auto-Negotiation	Enabled
LACP Mode	Disabled
Energy Efficient Ethernet	Disabled

TROUBLESHOOTING TIP

Most managed switches default to treating multicast intelligently via IGMP Snooping. The LogiCue NET System only uses the join/leave messages when cue lights join the multicast group (when the system first boots up). You must configure the switch to allow "unknown multicast" forwarding - otherwise, the switch will drop your multicast traffic after the membership timeout expires (typically 5-10 minutes).

The root cause is: IGMP Snooping enabled + Unknown Multicast blocked = Periodic timeout disconnects

The solution is NOT to extend the timeout - the solution is to disable the blocking of unknown multicast traffic.

NOTES:

- Menu names and exact terminology vary by manufacturer (Cisco, HP, Netgear, Dell, Ubiquiti, Netgear, etc.)
- Consult your specific switch documentation for exact menu paths
- Always save configuration changes to startup/running config