VALTORIS TECHNICAL RESOURCES

BROADCAST STORM DIAGNOSTIC REPORT

Official IT/OT Network Incident Documentation Template

1. INCIDENT & SITE DETAILS

Date of Inspection:	
Facility / Zone / Workcell:	
Inspecting OT Engineer:	
Affected PLCs / Equipment:	

2. OBSERVED OT NETWORK SYMPTOMS

- ☐ Modbus TCP / PROFINET connections dropping randomly
- ☐ SCADA screen freezing or showing delayed tag updates
- ☐ Ping times to the edge router spike to >100ms or time out entirely
- ☐ Router or gateway device experiences unexplained watchdog reboots
- ☐ Unmanaged switches are used to combine PLCs and IP Cameras

3. EDGE ROUTER HARDWARE DIAGNOSTICS

Cellular Router Make & Model:	
Peak CPU Utilization (%):	
Peak RAM Utilization (%):	
Uptime Before Fault/Reboot:	

4. WIRESHARK PACKET ANALYSIS (THE PROOF)

**Capture taken on the mirrored port or router's internal diagnostic interface.*
Filter used: `eth.dst == ff:ff:ff:ff:ff:ff or (ip.addr >= 224.0.0.0 and ip.addr <= 239.255.255.255)`

Peak Broadcast Rate (Packets/sec):	
Primary MAC Address Source(s):	
Suspected Rogue Device (e.g., Camera):	

ENGINEERING CONCLUSION & REQUIRED ACTION:

According to ODVA EtherNet/IP specifications, background broadcast and multicast traffic should safely remain under 100 packets per second (pps). The captured Wireshark data above indicates a **Layer 2 Broadcast Storm** originating from a flat network architecture.

To prevent the edge cellular router's CPU from processing irrelevant multicast traffic and crashing the remote SCADA link, the IT/OT department must immediately implement physical segmentation.

Action Required: Isolate the critical PLC traffic using Port-Based VLANs directly at the edge cellular router.