# Tech Tips

# Improving Reliability in Ethernet Control Networks


## SUMMARY

The proliferation of Ethernet-enabled devices on the factory floor —from PLCs to I/O modules all the way down to sensors — in support of the "Industrial Internet of Things" (IIoT), communications, and other data needs requires continued vigilance against Ethernet traffic disruptions that can have serious consequences for a control network. This Tech Tip provides a general overview of the types of potential Ethernet traffic "storms" that can occur and of some of the techniques that can be used to prevent and mitigate against each type.


## Overview

As control networks become ever-more reliant on Ethernet for communications, it is more important than ever to set-up, configure and operate your Ethernet networks properly to avoid the potentially serious problems that Ethernet traffic storms can cause. Although broadcast storms are the primary concern, multicast and unicast traffic can sometimes reach levels that can compromise control system performance. The most important step you can take to ensure the proper functioning of your network is to set it up the right way in the beginning. But even if you have configured your network properly from the start, there are other reasons that you might find yourself plagued by network traffic problems. This tech tip will help you understand the types of Ethernet traffic, the issues that too much of any type of traffic can cause, and some ways to mitigate against potential problems.

## Types of Ethernet Traffic

To diagnose network reliability problems, it is important to understand the types of Ethernet packets that may be transported by the network. There are three types of Ethernet network traffic that are common to any Ethernet network and essential to its proper operation: unicast, multicast, and broadcast.

- Unicast traffic: Ethernet packets addressed directly to the MAC address of a specific device.
- Multicast traffic: Ethernet packets whose destination address is a multicast group address. Ethernet devices that want to process these packets are configured to listen on a particular group address.
- Broadcast traffic: Ethernet packets whose destination address is the broadcast address. All devices connected to the same Ethernet network receive broadcast packets.

While all three types of Ethernet traffic are common to any Ethernet network, excessive traffic of any kind can cause problems for an Ethernet network, particularly for an industrial control network which typically has more limited processing power relative to an office network and is especially sensitive to large volumes of message traffic.

## Can There Be Too Much of a Good Thing?

Excessive Ethernet traffic is often referred to as a "traffic storm." The most common type of traffic storm is a broadcast storm, but both multicast and unicast traffic can cause issues for your control network as well.

Several modern Ethernet I/O protocols are based on multicast messages, and when a network contains large numbers of devices using multicast protocols, network loading can increase substantially. In situations where there are multiple SCADA systems polling for large amounts of data, even unicast message traffic can sometimes reach a level where problems can occur.

The following sections will discuss the different types of network traffic storms and ways to prevent and mitigate against each type. In order to determine which type of traffic (and which device) is causing your traffic storm, it is usually necessary to utilize a protocol analyzer or "packet sniffer" to capture and analyze network traffic. We at CTI prefer to use Wireshark, a free, open-source network protocol analyzer. While this paper will not attempt to provide further information on using Wireshark or any other network protocol analyzer, there is a wealth of information available on the Internet. One article we like is by Brian Hill at www.arstechnica.com/information-technology/2016/09/the-power-of-protocol-analyzers/.

## Unicast Traffic: How Can High Levels Affect the Control System?

The typical Ethernet-enabled PLC sees several sources of Unicast traffic, including:

- SCADA systems polling the PLC for data
- HMI panels polling the PLC for data
- Other PLCs polling for data
- PCs performing programming operations

Each Ethernet packet received by the PLC causes an "interrupt," requiring processor resources to remove the packet from the receive buffer and save it for processing later during the communications task. When high unicast packet rates occur, the PLC can spend considerable time in this "interrupt" processing. If the packet rate becomes excessive, larger and larger amounts of processing time are consumed, resulting in degradation of process control tasks and dropped Ethernet packets.

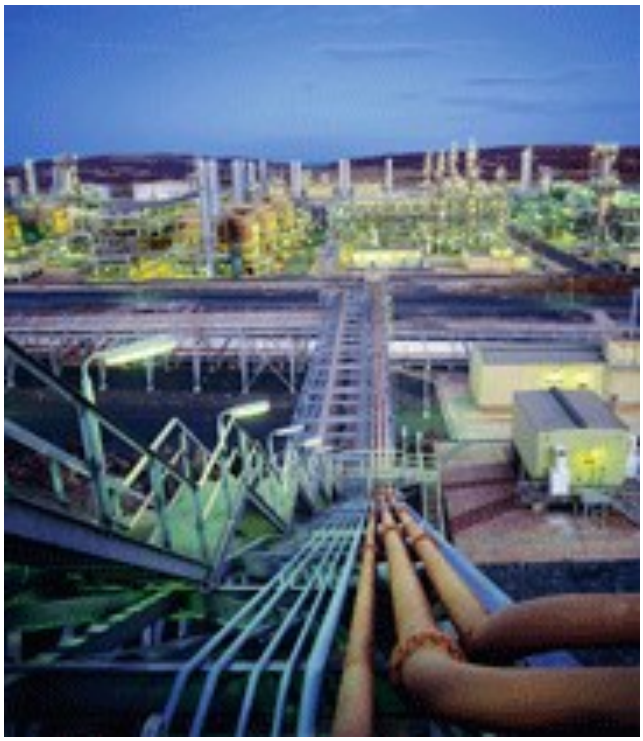
Ethernet switches learn the MAC address of devices communicating with each switch port. Once the MAC address is known, the switch forwards unicast packets with a given unicast destination only to the corresponding port. The network interface of an Ethernet device blocks reception of all unicast packets except for those whose destination address equals the MAC address of the interface. For these reasons, excessive loading due to unicast packets is less likely. Nevertheless, it is still possible under certain conditions, including the following:

- A large number of devices, such as SCADA/HMI systems, that are rapidly polling for data. While the average packet rate is often acceptable, traffic from these systems tends to be in bursts - a flurry of packets followed by a period with no packets. As the number of devices increases, bursts from multiple devices overlap, causing large traffic peaks.
- Misconfigured devices erroneously sending to the IP address of the device.
- Denial of Service (DoS) attacks, where a flurry of packets are sent to the unicast address in order to degrade operation.

## Mitigating Unicast Traffic Problems

Depending on your situation, the following actions can resolve unicast traffic problems:

- Reduce the polling rate of the SCADA/HMI systems, if possible. Most of these systems poll more rapidly than required (twice as fast as the required update time).
- Locate and reconfigure/disable any offending devices.
- Connect the device to a switch capable of rate limiting. Configure the switch to limit packet forwarding to an acceptable packet rate. Because rate limiting can buffer Ethernet packets, it can be used to level out traffic peaks.
- Use a CTI communications module, such as a 2572-B or 2500P-ECC1 for network communications.



## Multicast Traffic: A Commonly Overlooked Cause for Control Network Issues

Properly implemented, multicast messaging is an efficient communications method for your controls system when the same data needs to be transmitted to multiple recipients. EtherNet/IP often uses multicast for communications between the PLC and I/O devices.

However, in certain circumstances, multicast traffic can create problems. Multicast traffic tends to have higher packet rates than unicast traffic because there is no requirement to wait for a device to reply.

By default, Ethernet switches flood multicast packets to all switch ports, thus propagating these packets throughout the Ethernet network. Combined with high rates of multicast traffic (for example with EtherNet/IP I/O), this behavior can adversely affect the operation of network devices.

Most devices always allow some multicast traffic to pass through the Ethernet interface. This traffic includes packets with multicast addresses related to network control and multicast group management. Consequently, it is always possible for multicast traffic to cause interrupts on the device.

## Mitigating Multicast Network Problems

Multicast traffic will not present a problem for the CTI 2500 -Cxxx Processor: it does not support multicast and is configured to block reception of all multicast messages. To prevent unwanted multicast traffic from flooding other CTI products, you have several solutions. If you do not wish to use your CTI Ethernet-enabled products for multicast communications at all, you can connect them to a managed switch that supports IGMP (Internet Group Management Protocol) snooping (almost all do). This feature detects IGMP requests to join a particular multicast group and forwards the associated multicast stream only to the port connected to the requesting device. Most switches that support IGMP snooping can be configured to discard multicast streams that are unknown to the switch. If you want your CTI product to receive a multicast stream, however, this solution will not work properly, since it requires the CTI product to respond to an IGMP query from a router. Current CTI products will not respond to an IGMP query as they were designed for multicast communications on the local network only.

An alternate solution when you want your CTI product to receive multicast messages is to use a managed Ethernet switch that supports Bridge Multicast Filtering. This feature allows you to statically define how multicast packets are forwarded. If you want to receive multicast packets with a particular group address, you can statically assign the group address to the port. You can also choose to block all multicast packets from being forwarded to designated ports.

If you don't want to add an external switch, another possibility is to use a CTI product such as the 2500P-ECC1 and/or 2500P-ACP1 that employ embedded switches which limit the rate of multicast (and broadcast) packets. While this solution is often effective, there is some risk of missing packets that you want to receive, since the limiting algorithm begins discarding packets after the maximum threshold is exceeded.

A more global solution is to segment your Ethernet network, as discussed in the following sections.

## Broadcast Traffic: The Most Common Culprit for Network Disruptions

Broadcast traffic is required for proper operation of TCP/IP over Ethernet. For example, the Address Resolution Protocol (ARP), which discovers the MAC address of a device with a known IP address, is required in order to transmit TCP/IP unicast messages via an Ethernet link. As noted earlier, all devices on an Ethernet network must consume resources to process the broadcast packet. As more and more devices are added to the network, the number of broadcasts naturally increase.

Broadcast storms occur when an abnormally high number of broadcast messages are sent within a short period of time, overwhelming devices on the network and oftentimes causing congestion and dropped packets in the network switches.

While broadcast storms may simply be a nuisance in an office network, they can be catastrophic in a control network. Because of size, cost, and power constraints, devices in a control network typically have limited processing power relative to an office computer. In addition, those limited resources must remain dedicated to the primary control task to ensure proper equipment operation.

## What Causes a Broadcast Storm?

While there can be many factors that contribute to a broadcast storm, the most typical causes are the following:

**Combining the plant floor network with the IT network**
Information Technology (IT) networks often generate a lot of broadcast traffic. While this level of broadcast is acceptable for the IT network, it can seriously degrade the performance of control systems, which require real time operation.

**Excessively large control networks**.
Even when isolated from the IT network, large control networks themselves can generate too much broadcast traffic due to the number of devices attached to the network and the protocols employed.

**Poorly designed control protocols**
It is not unusual to find rogue Ethernet communications and I/O protocols that use broadcast as the primary means of delivering data. Typically these are legacy protocols that were developed in the early stages of Ethernet adoption.

**Hardware Failure/Defective Switches**
A defective switch, router or computer network interface can flood the network with broadcast traffic. It is worth it to invest in quality networking equipment that is equipped with storm prevention features.

**Human Error**
A common human error is when a loop is inadvertently created causing broadcast traffic to continually repeat through the network. A loop can be created either by connecting both ends of a cable into two ports of the same switch or by creating a loop among several switches.

## Preventing or Mitigating Broadcast Storms

There are several ways to reduce the occurrence of storms and/or to mitigate network disruptions caused by a storm.

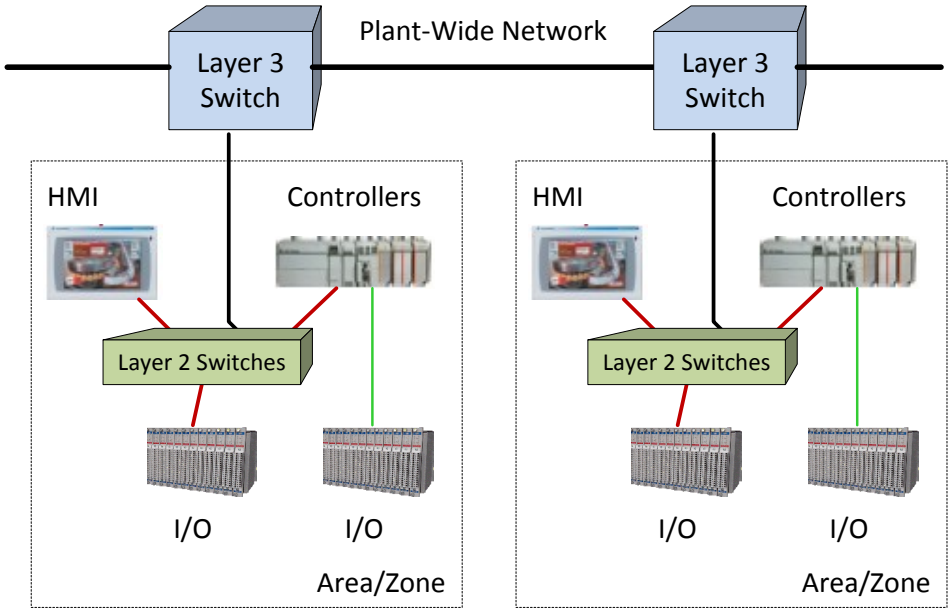
### 1. Isolate the IT Network from the Control Network

Ensure that your corporate IT network is either physically isolated from your controls network or is separated from it by properly configured routers and firewalls. Routers forward unicast and designated multicast TCP/IP packets but do not forward broadcast traffic. Firewalls further limit the TCP/IP packets that will be accepted. These network components allow communications between the administrative offices and plant floor while preventing broadcast and undesirable unicast/multicast packets from entering the control network.

### 2. Subdivide your Plant floor network into smaller segments

One of the best ways to tame broadcast and multicast traffic is to subdivide the network into smaller broadcast domains. Most plant floor environments can naturally be divided into work areas that are automated by one or more controllers and associated I/O. Each broadcast domain would consist of an isolated Ethernet Local Area Network (LAN), connected to the larger plant-wide network via a Layer 3 switch. The Layer 3 switch performs the function of routing TCP/IP packets between the LAN and the main network while also providing Ethernet switching functions (Layer 2). Consequently, broadcast packets from the larger network are not propagated to the LAN. (see *Figure 1* below).

*Figure 1: Subdivided plant network*.



### 3. Implement Broadcast Storm Control

One of the easiest and best ways to minimize the effects of storms and high packet rates is by installing a managed switch. All managed switches have the ability to set rate limits for broadcast traffic. Many others also enable rate limiting of multicast and unicast traffic. As an example, the illustration below (*Figure 2*) shows the Storm Control configuration web page for a Cisco 8-port managed switch. This switch allows setting of independent packet rate limits for broadcast, multicast, and unicast traffic. The rate limits are set as a % of the total network bandwidth or as packets per second (pps). For ports connected to CTI products, we recommend the port to be limited to 1000 broadcast/multicast packets per second (1% of a 100Mb link).

### 5. Training

To reduce human error, it is important to properly train all personnel who will be interacting with the network. Having a basic knowledge of network operation, including an understanding of the types of traffic storms and how to prevent/mitigate against them, can prevent errors, aid in recognizing typical problems, and improve the capability to accurately report anomalies to support personnel. Having technicians that can use a network capture program, such as Wireshark, to record network events can vastly improve the ability of CTI customer support personnel to assist with the resolution of a communications problem.

*Figure 2: Storm Control configuration page for a Cisco 8-port managed switch.*

Storm Control

**Storm Control Table**

| | | | Broadcast Storm Control | | | Multicast Storm Control | | | Unicast Storm Control | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Entry No. | Port | Mode | Threshold | Threshold Type | Mode | Threshold | Threshold Type | Mode | Threshold | Threshold Type |
| ○ | 1 | g1 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 2 | g2 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 3 | g3 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 4 | g4 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 5 | g5 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 6 | g6 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 7 | g7 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |
| ○ | 8 | g8 | Enable | 1000 | pps | Enable | 1000 | pps | Enable | 1000 | pps |

### 4. Implement Switch Loopback Protection

Many modern Ethernet switches provide a loopback detection feature, which prevents the inadvertent creation of a loop. The feature operates by periodically transmitting loop protocol packets out of a port that is enabled for Loopback Detection. If the same packet is subsequently received by the port, the port is automatically disabled, stopping packet loop propagation. Many of today's switches support Rapid Spanning Tree Protocol (RSTP) to keep the network topology loop-free when employing redundant networks. RSTP, loops and network redundancy are advanced topics not covered by this Tech Tip.

## Conclusion

Ethernet is continuing to revolutionize industrial control systems. As manufacturers explore the "Industrial Internet of Things" (IIoT) and implement more and more Ethernet-connected devices, it is ever more important to understand and manage the risk of Ethernet traffic storms. This Tech Tip provided a high-level view of the risks of traffic storms and some steps you can take to prevent or mitigate against them.

Please contact us if you need additional assistance.

**CONTROL TECHNOLOGY, INC.**
5734 Middlebrook Pike
Knoxville, TN 37921 USA
+1.865.584.0440
www.controltechnology.com
sales@controltechnology.com