Broadcast Storm Mitigation on Ethernet Networks
Executive summary

The intent of this paper is to explain what a broadcast storm is and how it can affect an Ethernet network. Mitigation techniques will be presented which can be used to reduce the chances of a broadcast storm occurring. A broadcast storm is an Ethernet network-level issue and when dealing with one the whole Ethernet network must be considered.
**Introduction**

Ethernet network traffic is classified as unicast, multicast, or broadcast traffic. Unicast traffic refers to a message being sent directly from one Ethernet device to another Ethernet device on the network. Multicast traffic refers to when one Ethernet device sends a message to a specific group of Ethernet devices. Broadcast traffic refers to one Ethernet device sending a message to all other devices on the network. All three types of Ethernet traffic are common to any Ethernet network and are essential to the proper operation of the Ethernet network. However a problem can arise when excessive broadcast traffic results in a broadcast storm.

Broadcast traffic by itself is a normal part of Ethernet network communications. One example of Broadcast traffic is the Address Resolution Protocol (ARP) message. Ethernet devices use ARP messages to resolve their IP addresses on the network.

Broadcast storms happen when a network is saturated with a large volume of broadcast traffic. They can occur for a short duration or for an extended period of time. Broadcast storms consume precious resources from every Ethernet device on the network. This is because every device needs to queue the broadcasts to be processed. Ethernet devices will also have to queue broadcast protocol messages that they do not support. In an Ethernet network, broadcast storms need to be reduced in order to minimize unnecessary CPU usage and to keep the network operating properly.
Causes of Broadcast Storms

There can be many contributing factors that can cause a broadcast storm. The most common are detailed below.

**Network design**
Ethernet networking is being implemented more and more in industrial environments as a control network. Often these control networks are linked to other networks such as the corporate IT network. It is highly recommended that the corporate and control networks are isolated from each other so that one does not influence the other. Corporate IT networks tend to have more broadcast traffic because of the wide variety of communication protocols that can take place on this type of network. Whereas Industrial control networks often are limited to one or two types of communication protocols.

**Defective or improperly configured Ethernet devices**
An Ethernet device which is defective or not properly configured can also lead to a broadcast storm on the network. Some Ethernet devices are preconfigured to use many different networking protocols such as IPX, NetBEUI, and many others. Each of these protocols communicates via broadcast messaging which can increase the chances of a broadcast storm occurring.

**Human Error**
Broadcast storms can also be caused by human error. The most common error is when both ends of a cable are connected into two ports of the same switch. This causes a loop back condition in which broadcast traffic can be constantly repeated throughout the network.
Methods of Prevention

There is no way to completely eliminate the chances of a broadcast storm, but there are ways to reduce the risk.

Refining the design of the Ethernet network
Communication broadcast messages are far more common on a corporate IT network than they are on an industrial control network. Ideally an industrial control network should be physically isolated from the corporate IT network as well as the Internet. If physically isolating the networks is not an option, then devices such as routers or firewalls can be use to provide isolation of the networks. A router does not allow MAC level broadcast frames to pass into different networks. This can help reduce the chances of a broadcast storm on the corporate IT network from affecting the industrial control network. Firewalls can also help to prevent hackers from infiltrating the network and causing a broadcast storm. A simplified example of isolating a control network from a corporate network using a router and firewalls is shown in Figure 1.

Proper device configuration
Most Ethernet plug and play devices support multiple protocols and frame types. Although this offers convenience with peer to peer communication between Ethernet devices on the network, it can also increases the chances of a broadcast storm by causing an increase in the amount of broadcast traffic. The Ethernet network should be examined to see if all devices can communicate using a single protocol and frame type. Protocols and frame types that are not needed on the network should be disabled on all Ethernet devices in the network. It is also recommended that if any devices are not physically present on the network then every effort should be made to exclude these devices at the application level.
Industrial managed switches have features that can also help reduce the chances of a broadcast storm. Rapid Spanning Tree Protocol (RSTP) can be used to help eliminate the possibility of a loop being accidentally created and a resulting broadcast storm. RSTP will also find a new communication path between devices if one exists along the switch network in the event the initial path is lost.

In some industrial control networks there is a need for redundancy among the switches. To achieve this, switches along the network are generally connected in a loop or ring. This can lead to broadcast storms unless the switches support a redundancy management protocol such as the Media Redundancy Protocol (MRP) or HIPER-Ring protocol. These protocols utilize a redundancy manager (RM) to manage the ring. The RM has a main link and a redundant link on the ring. The redundant link will only pass Ethernet traffic if the RM detects a fault and enables this link. These protocols can help reduce the risk of a broadcast storm because the RM prevents a loop from being created. The basic topology for these protocols is shown in Figure 2.

For an industrial control network it is recommended that only Ethernet managed switches such as the ConneXium series be used. ConneXium Managed switches have a feature called broadcast filtering which is used to limit the amount of broadcast packets sent out of the switch ports. Since some broadcast traffic is essential to the continued operation of the Industrial Ethernet network, not all broadcast traffic should be filtered. Before using broadcast filtering the user must fully understand their Ethernet network. Setting the filtering limit too high can lead to many broadcast messages being process by the connected Ethernet device. Setting it too low can prevent necessary broadcast messages from reaching the connected Ethernet device. The amount of broadcast packets to be filtered will be heavily dependant on the Ethernet traffic of the network. When setting broadcast filtering the amount chosen will be the total number of broadcast packets allowed out of that Ethernet port per second.

**Reducing human error**

Human error can sometimes lead to a broadcast storm on the Ethernet network. The best way to prevent this is to properly train anyone who will be installing or maintaining, the network. Proper training can consist of, but is not limited to, educating the users on what broadcast storms are and their effect on the network, educating users on how to properly use and configure the devices on the Ethernet network, and providing useful documentation to the users.

---

**Figure 2**

MRP or HIPER-ring topology
Conclusion

Broadcast storms have multiple causes and it may be impossible to completely eliminate them. When a broadcast storm occurs, it affects all the devices in an Ethernet network. By following the information provided in this document, the chances of broadcast storms occurring and impacting equipment can be reduced.

- Isolate industrial control network traffic from corporate IT network traffic by using routers and/or firewalls.
- Make sure all Ethernet devices on the network are properly configured and utilize any features which can reduce the effects of broadcast traffic such as RSTP.
- Provide training to anyone who will be installing, or maintaining, the Ethernet network.

A broadcast storm is an Ethernet network level issue and when dealing with one the entire Ethernet network must be considered.