N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353

Using N-Tron's 500 Series Switches With Rockwell Automation's EtherNet/IP™

Warren Nicholson, Tom Sills, & Gordon Stevens

Introduction

This application note will explain how switches utilizing IGMP snooping can significantly reduce traffic from bandwidth-intensive IP multicast traffic generated by Rockwell Automation products. Additionally, it will describe the Internet Group Multicast Protocol (IGMP).

N-TRON is now shipping out of the box plug-and-play firmware in all current (Release 8+) 500 Series Switches purchased with the -A option. IGMP and query auto detect modes are now enabled by default, and key enhancements include multiple router support as well as dynamic router discovery and master/slave redundancy for query detection. These new features allow for the automatic detection of bi-directional router ports needed for the seamless formation of IGMP groups in EtherNet/IP™ environments. This will greatly reduce or eliminate the switch configuration requirements for most Ethernet control networks, dramatically saving time in configuring, commissioning, and maintaining Ethernet based control systems.

The automatic features may be overridden to provide manual configuration in the event noncompliant legacy Ethernet devices are present on the network. Lastly, this paper will discuss Port QoS and how it can improve determinism and reduce latency when used with Rockwell Automation's PLC's.

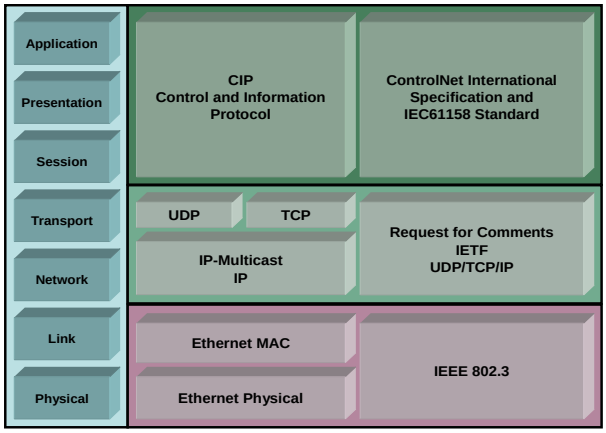
EtherNet/IP™

Rockwell Automation EtherNet I/P devices support two distinct message types - 'explicit' messages and 'implicit' messages. 'Explicit' is a point-to point, request/response (client/server) protocol typically used for unscheduled "information" messaging, while 'implicit' is a multicast, producer/consumer protocol designed for scheduled "control" data transfer. The term "explicit" refers to an address which explicitly details the path to a specific target object.

Explicit messages are information messages used for device configuration and diagnostics, which are highly variable in both size and frequency. With explicit messaging, nodes must interpret each message, execute the requested task, and generate responses. On the other hand, Real-time control or 'implicit' messaging demands different performance. Here, the protocol needs to be able to support multi-casting (send to a number of nodes), while ensuring processing time in the node is kept to a minimum. This is due to the time-critical nature of the transfer.

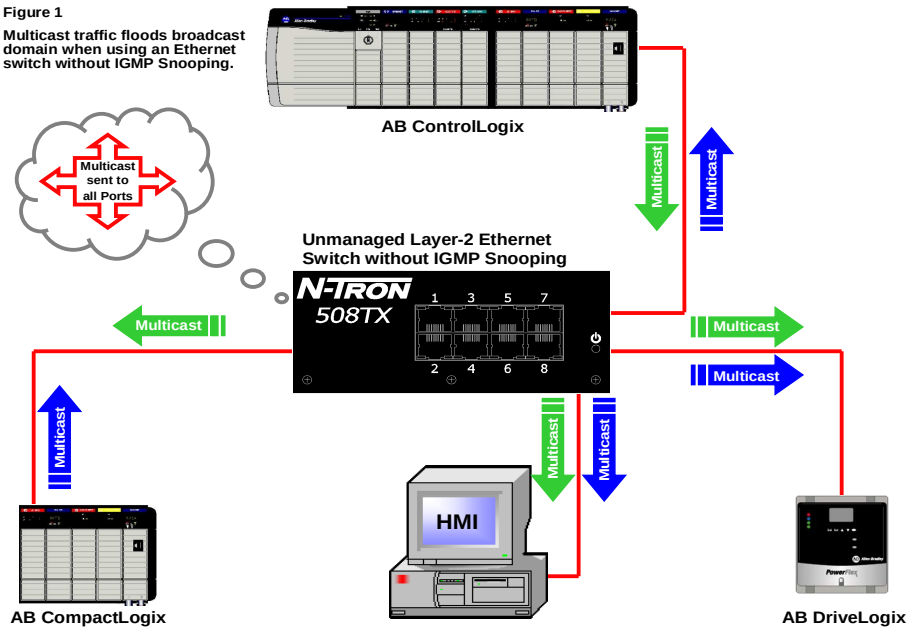
EtherNet/IP realizes explicit messaging by using TCP/IP encapsulation. With this approach, the data field carries both protocol information and instructions for service performance. EtherNet/IP employs a different protocol to realize implicit messaging - the User Datagram Protocol/Internet Protocol (UDP/IP). The UDP/IP data field contains no protocol information, only real-time I/O data. The meaning of the data is predefined at the time the connection is established and processing time in the node is therefore minimized during runtime. Such messages are low overhead, short, and provide the time-critical performance required for control functionality.

N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353



By using both TCP/IP and UDP/IP protocols to construct network messages, both implicit real-time I/O and explicit messaging can occur. When using this methodology, EtherNet/IP allows prioritization of I/O data over regular non time-critical messaging data. As a result, EtherNet/IP supplies every service that is essential in control and device-level networks - from polled, cyclic and change-of-state trigger mechanisms to multicast and point-to-point data transfer. This provides Ethernet users with real-time I/O, device-configuration and diagnostic capabilities, along with the interoperability and interchangeability demanded by modern industrial applications.

Figure 1
Multicast traffic floods broadcast domain when using an Ethernet switch without IGMP Snooping.



Layer-2 Switches and Multicast Packets

By default, an unmanaged layer 2 Ethernet switch floods multicast traffic within the broadcast/multicast domain. This consumes a lot of bandwidth if several multicast servers are sending streams to a LAN segment. Multicast traffic is flooded because a switch usually learns MAC addresses by looking into the source address field of all the frames it receives. However, a multicast Group Destination Address (GDA) MAC address (01:00:5E:XX:XX:XX) never appears as a source address for a packet. Therefore a layer-2 Ethernet switch cannot “learn” the port associated with source of the multicast packet, hence it must forward the multicast packet to all ports.

N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353

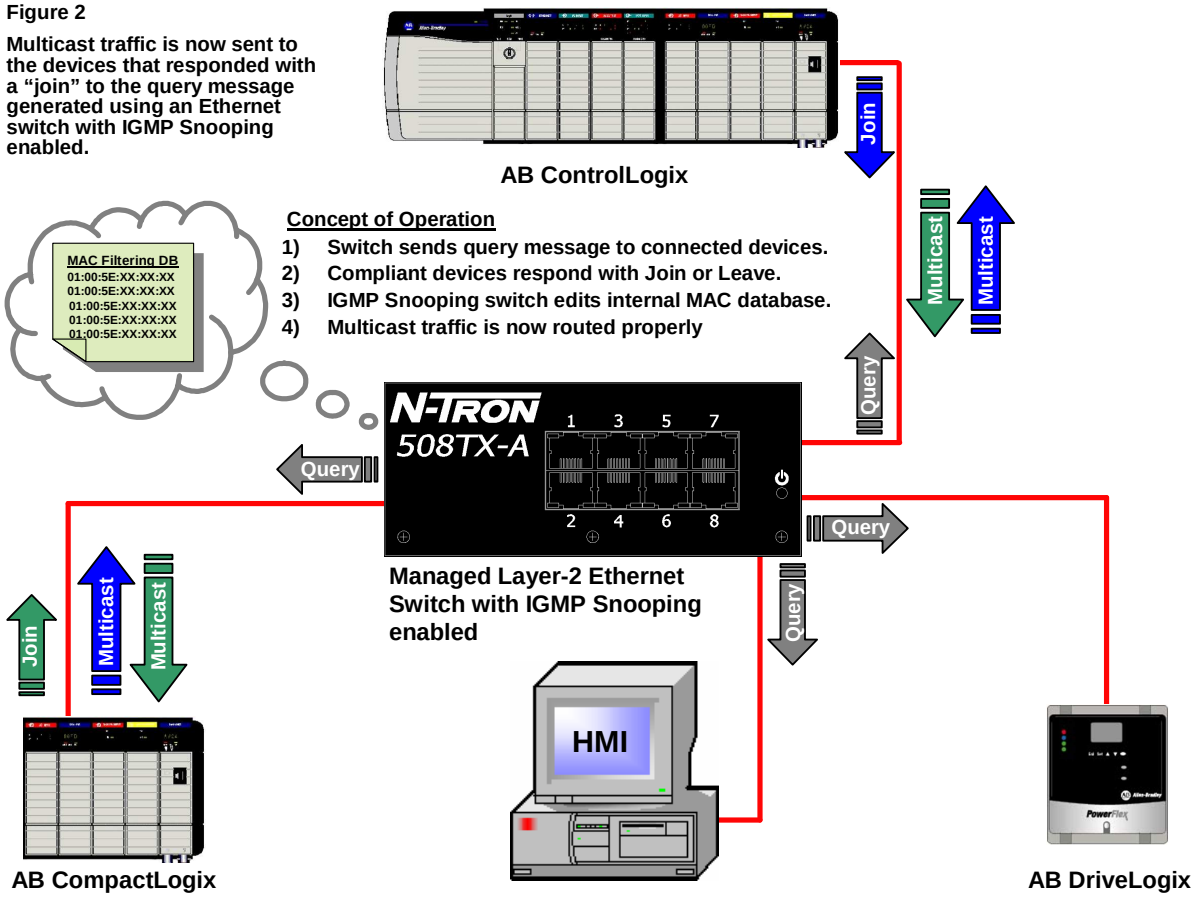
IGMP Overview

IGMP protocol starts with a query packet. According to the RFC's the router with the lowest IP address on the network is responsible for generating the IGMP query packet. All nodes that support IGMP require a querier to be present on the network (EtherNet I/P is no exception). The use of routers for this purpose is often not desired in a stand alone control systems environment due to the delays they create in communication and added expense. N-Tron switches do not require the use of a router by providing the configuration option to enable the switch to generate query packets.

In response to the IGMP query packet, participating nodes will respond with the appropriate Join or Leave messages. Unsolicited (early) joins or leaves are also supported by N-Tron's implementation of IGMP. If a node joins a group, the address is added to the MAC filtering database. If a node leaves a group, the address is removed. EtherNet I/P implicit messages generate multicast IGMP packets that could impact the determinism of a large network by loading it down with multicast traffic. Managed switches that support IGMP Snooping have the capability to "learn" IGMP group members, and "route" multicast traffic intelligently, instead of flooding.

Figure 2

Multicast traffic is now sent to the devices that responded with a "join" to the query message generated using an Ethernet switch with IGMP Snooping enabled.



Joining a Multicast Group

When a host decides to join a multicast group, it sends an IGMP Report message to the GDA it wants to join. The IGMP snooping switch will recognize the IGMP Report message and add a GDA MAC address of the associated port in the MAC Filtering Database. When multicast traffic is transmitted to the switch, it will forward the traffic to the ports associated with this GDA MAC address regarding the Filtering Database.

N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353

Switch Configuration, not necessary in most cases:

All current 500 series –A switches now include:

- **Out of box Plug-and-Play with most Ethernet control networks, especially suited for EtherNet/IP networks**
- **Automatically discovers other *N-TRON* multiple switches and registers their interconnected ports as IGMP router ports**
- **Dynamic router discovery algorithm**
- **Dynamic IGMP query discovery algorithm**
- **Master/Slave query redundancy for IGMP based control networks**
- **Reduces or eliminates Ethernet switch configuration for control networks**

In order to possibly adapt to special circumstances or legacy devices, manual configuration options are provided in current 500 series –A switches:

- In addition to the out of box default of auto-detection of router ports, any number of ports can be manually set as router ports, for use with less intelligent switches. This setting will be remembered though power cycles. Most IGMP capable switches that issue queries will be auto-detected in normal conditions, but if a port is not manually set as a router port then switches other than N-Tron's may not remain properly acknowledged after link drops and restores, or through power cycling of various network components. N-Tron switches out of box automatically recover from these events.

- The query management function enables the switch to generate IGMP "Query" messages: never, always, or automatically. This setting will be remembered though power cycles. The default out of box is automatic. In automatic, in the steady state, only one N-Tron switch will be issuing queries over time, but if that one stops for any reason another N-Tron switch will pick up the querier task automatically in a timely manner.

Router Data Filter

According to the IGMP RFC's, the router port should receive all IGMP packets. This strict implementation can result in unnecessary data traffic on the uplink/router port. The N-Tron 500 Series –A implementation (Designed in conjunction with Rockwell Automation), provides an option to filter the IGMP data packets selectively by port from the router port(s), and thus reduces unnecessary network loading in certain circumstances. IGMP Join and Leave control messages will still be sent to the router regardless of this setting. One example use of rfilter could be a ring on which the IGMP data is not needed because the devices communicating using IGMP are on the same leg beneath the ring. Out of box, all router ports (if there are any) will receive IGMP controls (joins, and leaves), but will not receive any IGMP group data unless a join for that IGMP group has been received into that port. That is, with rfilter on router ports will not get IGMP data just by being a router port, but can if a join came into that port for that IGMP group. On the 500 Series –A Switches, rfilter can be enabled or disabled for any number of individual ports, and if enabled, router ports get the IGMP control frames, which are small and infrequent, but do not get the IGMP group data. This setting will be remembered though power cycles. For each port rfilter will have an impact only if that port is manually or dynamically chosen as a router port. Rfilter is enabled on all ports in factory defaults.

Port QoS

Port Quality of Service (QoS) provides an effective way to assign high priority to the traffic entering from the ports you designate. By default, all ports will have the same priority status assigned. Therefore, without the use of Port QoS, the switch will process all packets in the order in which it received them. In the current 500 series –A switches, Port based QoS is disabled by default and can be enabled by selecting any number of ports. Typically, the ports that have a device connected, such as an AB ControlLogix PLC controller, would be selected for this feature. Once enabled, the traffic received on the ports you designated is given higher priority and will be processed before the lower prioritized traffic. Port

N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353

QoS is especially useful when using legacy devices that are not IGMP compliant. This feature will allow you to further control latency and determinism in a controls network environment that may be loaded down with multicast messages. NOTE: port QoS will override 802.1p tagged QoS.

N-Tron Ethernet Switch Configuration

Manually setting router ports

By default, IGMP is already enabled out of box in all current (Release 8+) 500 Series Switches purchased with the -A option. In factory defaults the router mode is auto with no manual ports selected. Our out of box IGMP Snooping feature will prevent the unnecessary multicast traffic on the LAN from overloading the network in most cases. However, you may have some devices that are not IGMP aware. In these cases, you can manually enter static filters to achieve the same results. This will over-ride the dynamic IGMP Snooping when conflicts exist.

On a current (Release 8+) 500 series –A switch, to manually configure the router ports, you will need to perform the following steps:

1. Connect a standard serial cable to the COM port and load a terminal program on the PC.
2. Supply power to the switch.
3. Press [ESC].
4. When prompted to do so, log in with User Name: admin [ENTER].
5. Enter the Password: admin [ENTER].
6. Type SWITCH and press [ENTER].
7. Type IGMP and press [ENTER].
8. Type ROUTERS and press [ENTER].
9. Type A, or M (see below) and press [ENTER].
10. Type in the port numbers to be manually selected router ports when prompted and press [ENTER].

Example of the IGMP router management screen:

```
CLI\SWITCH\IGMP>routers

For IGMP Snooping, router ports mode is auto.
Manually Selected Router Port(s): none
Automatically detected Router Port(s): none

Enter:  <(ESC)> to keep this configuration, OR
      'A' to Auto-detect plus manual, OR
      'M' for Manual only, OR
      'N' for None.
```

Example of entering manually selected routers in auto-detect plus manual:
(**One does not have to manually enter anything for IGMP SNOOPING**, unless accommodating non-IGMP devices.)

```
Enter A, M, N ,  (or ESC to exit) > a

For IGMP Snooping, router ports mode is auto.
Manually Selected Router Port(s): none
Automatically detected Router Port(s): none

Would you like to change that ?   Enter 'YES' or (NO):
CLI> yes

Enter ports to be router ports:
Use commas to separate port numbers.
(Example: '3,6,12,14<enter>'.)
Enter Port Numbers (or ESC to exit)> 1,8,17

CLI\SWITCH\IGMP>
```

11. Cycle power to the switch to initiate new settings.

N-Tron Corp.
820 S. University Blvd. Suite 4E, Mobile, AL 36609
PH: 334-342-2164 • FAX: 251-342-6353

Enabling Port Quality of Service QoS

By enabling the Port QoS, the N-Tron switch will assign high priority to the traffic it receives from the ports you select.

To enable the Port QoS on 500 series –A Switches, you will need to perform the following steps:

1. Connect a standard serial cable to the COM port and load a terminal program on the PC.
2. Supply power to the switch.
3. Press [ESC].
4. When prompted to do so, log in with User Name: admin [ENTER].
5. Enter the Password: admin [ENTER].
6. Type SWITCH and press [ENTER].
7. Type QOS and press [ENTER].
8. Type SET_PORT and press [ENTER].
9. Enter the ports that you want to designate with high priority as prompted and press [ENTER].
10. Type EN_PORT and press [ENTER].
11. Type INFO [ENTER] to verify your configuration.
12. Cycle power to the switch to initiate new settings.