I.J. Wireless and Microwave Technologies, 2012, 6, 10-16
Published Online December 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.06.02

Available online at http://www.mecs-press.net/ijwmt

A New Solution of Multicast Packets Management for Managed Ethernet Switch

Sheng LU

School of Computer Science and Information Engineering, Chongqing Technology and Business University, Chongqing, China, 400067

Abstract

This paper has a discussion on the new solution of IGMP management for multicast message in industrial Ethernet. It proposed a new mechanism to minimize the congestion which is based on the taking an adaptive decision during transferring multicast messages. Proposed approach is that a device requesting to start and stop the reception of the multicast streams is accomplished through IGMP join and Leave message requests. Quality of Service (QOS) as a component is supported by the Switch Manager as well as features built into the micro chip. The IGMP Snooping component monitors (snoops) these join and leave messages to allow it to know which streams to prune from which ports. it is a service provided by most managed Ethernet switches. However, the ICIE (Intelligent Controller for Industrial Ethernet) does not provide this capability and requires that another device in the network supports the querier functionality. It is through the external devices solicitation of join messages that allow the IGMP Snooping component to correctly decipher on which ports the downstream listeners are connected.

Index Terms: IGMP; industrial Ethernet; switch management; Qos

1. Introduction

Nowadays, more and more network applications, such as data distribution, distant education and distributed database, work on the multicast communication mode.

As one of the most important elements of streaming architecture is control the network traffic. Network traffic evolves issues like rate control also called as flow control or congestion control. It is very crucial to resolve congestion state to maintain the flow of streams. It is important to control multicast packets for Ethernet switch. Congestion becomes more important at the multicast scenario where the entire receiver may have capability to adapt different bandwidth [1].

* Corresponding author.
E-mail address: lusheng8815@126.com

Multicast Congestion control can be handle by router or end to end entity which may be done by source based approach as well as receiver driven approach. Source based approach is not much efficient and can not handle heterogeneous receivers. Receiver driven approach based on concept that all active decision is taken by receiver. This approach use layered transmission technique in which incoming stream is divided into different layer depend on the QoS requirements.

Every IP host in Ethernet has a unique 32-bit IP address. The IP address is interpreted in three logical parts, namely, class, netid and hostid. In our discussions, we are only concerned with the Class-C and the Class-D IP addresses. For a class-C host, the IP address remains fixed since the point of attachment to IP network for such-a host does change. When a host roams from one IP sub-net to another, IP man-dates that the IP addresses for the host remain fixed despite the fact that the point of attachment of such a host to the network may keep changing. When the IP address of the node does not change, its remains "transparent" to the hosts communicating to it. Multicasting represents an efficient means for using the network resources for one-to-many communication. Deering first described IP Multicasting in his doctoral dissertation.

Since IP multicast packets are directed to a multicast group with a specific class-D address rather than a specific host, any particular host may receive or send such packets after joining the associated multicast group. As long as multicast IP packets are able to arrive at the IP sub-net-being visited by a host, it is not necessary to track the location of a IP host or tunnel multicast packets. A host may simply issue new join requests over the IP sub-network being visited and issue leave group requests at its previous point of attachment.

The IGMP is used for joining, leaving and managing IP multicast groups. IGMP in its present form allows only one group to be handled at a time. For example, if a host was a member of multiple different multicast groups, it would need to send as many IGMP 'leave' packets in order to leave these multiple multicast groups. A set of multiple join request packets to re-join these groups from within the new IP sub-net will follow this [2].

In this paper, we propose a new solution of multicast packets management for Managed Ethernet Switch to send aggregate leave and/or join request packets. In the above example, the modified IGMP would require only a single packet to send the join request for the entire multiple multicast group that a host wishes to re-join.

For the future merge of networks, the computer network needs the multicast capability to support the traditional industrial message Broadcast business. So how to support the multicast communication in the network is the network researcher's important direction. Over the Internet, the IP Multicast has been implemented and used for a long time. But multicast in the Intranet has not got the same rapid development.

2. Quality of Service

Quality of Service (QOS) as a component is supported by the Switch Manager as well as features built into the Marvel 88E6165. It is designed to meet ODVA recommendations. QOS utilizes the four traffic classes in the queue controller as shown in Figure 1 to prioritize and deliver traffic through the switch fabric enabling a network designer to increase the reliability of high priority traffic [3].

ICIE (Intelligent Controller for Industrial Ethernet) products implement QOS using Differentiated Services (DiffServ), also known as DSCP, using a 6 bit value in the TOS field of the IP header to mark frames with the differentiated priorities. Since the overall frame format is unchanged this form of tagging continues to work with devices that do not support QoS.

On ICIE modules with QOS enabled, outbound Modbus TCP and EIP packets will be tagged with their appropriate priority prior to being transmitted onto the network. The QOS configuration of the ICIE modules allows the tag values (DSCP tag) of Implicit and Explicit Messaging to be configured by the user; although the default values are as recommended by ODVA [4].

The internal switch of the ICIE provides priority handling of traffic based upon the DSCP values. The switch provides four levels of queuing from highest priority to lowest priority as follows:

3. Management traffic – RSTP and IGMP,
2. High priority traffic,
1. Low priority traffic,

0. All other traffic.

Each port has a set of four queues to allow packets to be prioritized prior to transmit. As packets arrive at the switch of the ICIE they are classified according to a DSCP tag-to-queue mapping table. The packets are then placed into the appropriate queue on their destination port; be it either the internal port or one of the external ports. They are then transmitted out of their destination port according to the priority of the queues.

For the ICIE with its built in switch, QOS tagged packets that are destined for the module as well as packets that are passing through the module to some other device will be handled according to the QOS priority scheme. The DSCP tag values associate the message stream to one of the four priority queues. Changing the values will not only affect the tagging of outbound frames but will also re-associate the new DSCP tag values with the appropriate queue. Normally the default values should suffice; however, if a network is using a conflicting QOS tagging scheme the DSCP values may be changed to match. The user has the ability to configure both the priority tagging of the Modbus and EIP traffic as well as the mapping of this traffic into one of the switch queues. Any packet that is not tagged will go to the lowest priority queue. An untagged packet is essentially the same as having a DSCP value of zero. Therefore, untagged Modbus TCP and EIP traffic will be treated at the lowest priority.

For compliance with ODVA requirements the QOS parameters must be configurable via the network with a CIP request using the QOS object. In addition, these parameters must be persistent through a reboot. To accommodate these requirements, a "QOS From Flash" flag will be used in the configuration from the PLC to indicate that the device should obtain its QOS configuration from its local flash. If this bit is set, upon receipt of a QOS object the ICIE modules will save the parameters to local flash; otherwise the modules will return a CIP error response. Upon restart, if the "QOS From Flash" bit is set in the PLC configuration, the module will take the QOS configuration from flash if it exists. If it does not exist the modules will use the default values.

Therefore the component needs only concern itself with initialization and configuration and provide an interface for other components to get the DSCP values they need to tag their type of packet.

3. Network Topology Architecture

This section simply analyzes the potential network topologies in which our customers may use the ICIE module and how the ICIE module's architecture facilitates these topologies.

A. Simple Network Topology

Figure 1 shows a simple network topology which is a combination of the bus network topology, star network topology, and tree network topology. The "simple" means that there are no loop and daisy chain in which the ICIE module involves. All the ICIE modules can be used in this topology network [5].

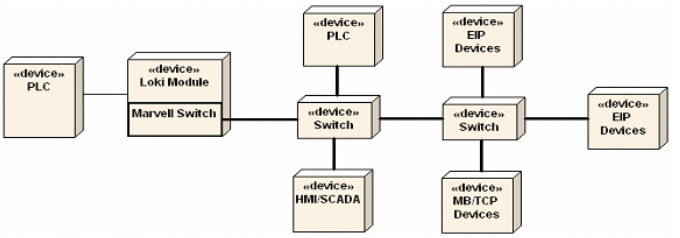

Figure 1. The simple network topology of the ICIE control network.

Because of no loop in the simple network topology, the RSTP functionality can be disabled to save the bandwidths of the ICIE CPU and the network and reduce network traffics. Therefore, this version of the ICIE module architecture should allow the users to enable or disable the RSTP feature as they need and the default

setting for the RSTP feature should be enabled. But the IGMP Snooping and QOS features should be enabled to improve the performance [6].

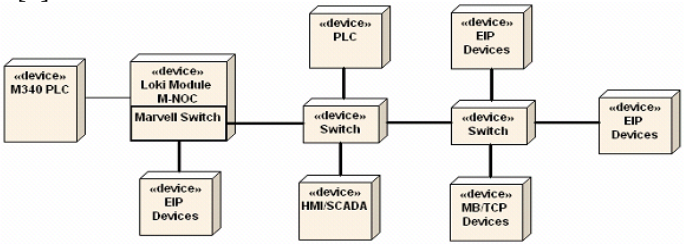

Figure 2. The simple network topology with the ICIE module.

In the simple network topology, the ICIE modules as the communication modules for their corresponding PLCs can only be used as end devices; the ICIE module can act as an end device and/or a switch as shown in Figure 2.

B. Switch Ring Topology

Figure 3 shows a simple switch ring network topology in which the ICIE module involves in the ring as a switch and the enhanced RSTP is the topology maintaining protocol. This simple ring topology is typically used for reducing the cost of cable links when the devices are geographically distributed [7].

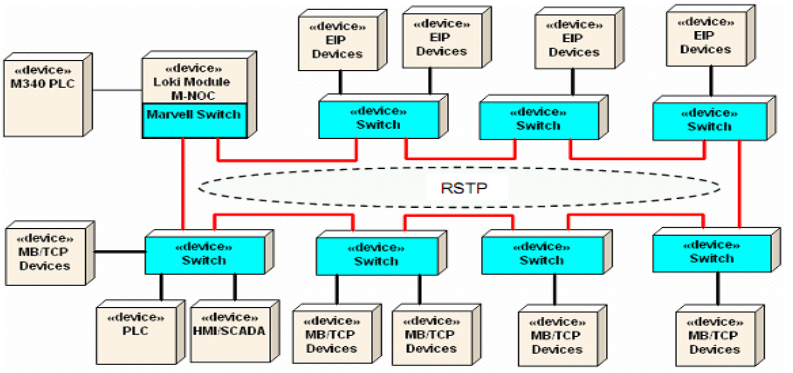

Figure 3. The switch ring network topology with the ICIE module.

In this topology, the fault recover time is mainly determined by the network infrastructure switches the users choose, not mainly by the ICIE module, and varies with the number of the switches in the ring and where the failure occurs. The worst case recovery time occurs when the switch just next to the root switch fails [8]. In the worst case, the RSTP TCN message transverses all the switches in the ring in one sequence. The best case recovery time occurs when the switch which is the farthest from the root switch fails. In the best case, the RSTP TCN message transverses all the switches in the ring in two sequences (each of which has half number of the switches) in parallel. Each switch needs to process the TCN and transmits it to the next switch and the time involved is called propagation delay (about 2-5 ms for managed switch).

In order to reduce the recovery time, the users may employ some other complicated ring topologies which will not be addressed here.

Because any 2 of the 4 external Ethernet ports of ICIE module can be used by the user to connect to the switch ring, this version of the ICIE module architecture allows the users to configure the switch ports through Unity

Pro and Web page. In this topology, the IGMP Snooping and QOS features should be enabled to improve the performance.

4. Multicast Packets Management

C. IGMP snooping service

The IGMP Snooping service of our product (Intelligent Controller for Industrial Ethernet, ICIE) provides a method to filter multicast traffic to downstream devices. The filtering consists of blocking the multicast traffic on ports to which there are no downstream consumers – a process known as "pruning". As a down stream device on a port registers for a particular multicast stream – an Ethernet/IP listen only connection for example – the IGMP Snooping component recognizes that a device in the direction of this port is requesting to receive the particular multicast traffic and allows the traffic to flow out of the port. On another port, however, if no downstream device requests the traffic, the IGMP Snooping component will cause the embedded switch to block this multicast traffic to the port. In this manner, ideally, only devices requesting this traffic receive this traffic [9].

D. Working process

The process of a device requesting to start and stop the reception of the multicast streams is accomplished through IGMP join and Leave message requests. The IGMP Snooping component monitors (snoops) these join and leave messages to allow it to know which streams to prune from which ports. This process uses a device performing a manager role to periodically query all devices in the subnet and subsequently cause them to re-join the multicast group of listeners for any stream in which they may be interested. The management role is known as an "IGMP Snooping Querier" (from now on known as the "querier") and it is a service provided by most managed Ethernet switches. The ICIE, however, does not provide this capability and requires that another device in the network supports the querier functionality. It is through the external devices solicitation of join messages that allow the IGMP Snooping component to correctly decipher on which ports the downstream listeners are connected [10].

In a situation where the querier device is not known, for example when the ICIE first boots, all multicast traffic is flooded to all ports – nothing is pruned. Eventually the querier device will send queries into the network to request that devices refresh their registration to multicasts groups via join messages. According to RFC2236, the default query interval should be 125 seconds. The IGMP Snooping component forwards the received query messages to all ports, except the port on which it was received, so that devices downstream will know that they must refresh their multicast group memberships. It is through snooping of these query messages that the IGMP Snooping component learns of the existence of a querier. Moreover, by keeping track of the port on which the query was received, IGMP Snooping learns the "direction" towards the querier [11]. Similarly, as devices downstream begin to request multicast traffic by sending the requisite join messages, the IGMP Snooping component learns also of the multicast groups that are being requested on each port. The IGMP Snooping component then forwards the join message toward the querier to allow the next device up the line (ICIE, switch or other device) to know that there are consumers on this link for the multicast stream in question. As a result, all join messages propagate toward the querier device. Since knowledge of the querier allows the IGMP Snooping component to correctly forward join messages, it is sufficient for IGMP Snooping to know only the direction toward the querier; the identity of the querier is not important.

E. Application architecture

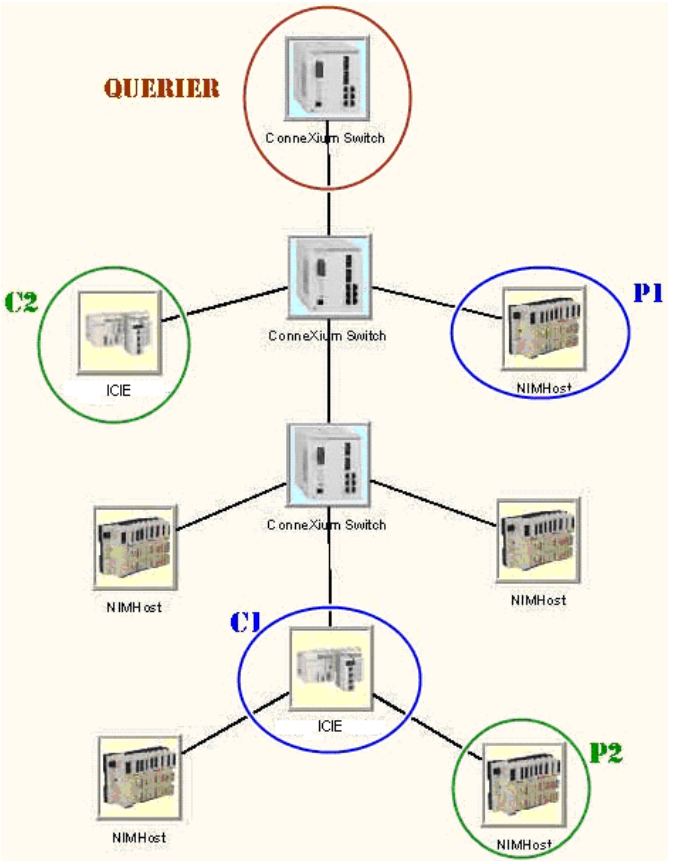

Figure 4. Network architecture

Figure 4 is the network architecture of IGMP application. Consider for a moment the case of a multicast producer (P1), an Ethernet/IP class 1 connection for example, in the middle of a network as shown in the diagram below. At the "top" of this network resides a switch acting as a querier. Since join messages propagate from the edge, or "bottom", to the top and consuming nodes (C1) below the producer have sent their join messages up, the switches along the way all know how to forward the multicast stream to these devices [12].

What about consuming devices (C2) "above" the producer (P2)? Since all join messages are only propagated up toward the querier, the ports on devices that point toward the querier have not seen any join requests for the multicast stream come down into that port. Without any further action, since the switch has not seen any consumers for the multicast stream in the direction of the querier, the multicast stream would be pruned from that port. Therefore, it is required that all multicast streams be forwarded toward the querier as well. Now for switches that are above the producer and have seen join requests come in on their ports pointing toward the edge, the switch can forward this stream toward those devices [13].

5. Conclusions and Perspective

Ethernet is the most common Intranet and access network. Previous Ethernet is a network shared by all hosts. It can't support the group communication. So Multicast is treated just as Broadcast. Now the switch Ethernet

with industrial Ethernet capability can support the TRUE multicast. By using industrial Ethernet, the switch Ethernet can separate the network into several broadcast domains. In case of a multicast traffic, only those hosts in this broadcast domain can send and receive the multicast data. Compared with the IP Multicast, the Multicast over Switch Ethernet does not need to support the Multicast Route function. It only needs a Dynamic Group Management Protocol to manage the relations between hosts and multicast groups.

We proposed a new mechanism to manage multicast packets to minimize the congestion which is based on the taking an adaptive decision during transferring multicast messages. Proposed approach is that a device requesting to start and stop the reception of the multicast streams is accomplished through IGMP join and Leave message requests. The IGMP Snooping component monitors (snoops) these join and leave messages to allow it to know which streams to prune from which ports. This process uses a device performing a manager role to periodically query all devices in the subnet and subsequently cause them to re-join the multicast group of listeners for any stream in which they may be interested. The management role is known as an "IGMP Snooping Querier" and it is a service provided by most managed Ethernet switches. However, the ICIE does not provide this capability and requires that another device in the network supports the querier functionality. It is through the external devices solicitation of join messages that allow the IGMP Snooping component to correctly decipher on which ports the downstream listeners are connected.

References

[1] ETRI, TTA, "Specifications for 2.3GHz band Portable Internet Service", Apr.2004.
[2] A.Dutta,J. Chennikara,W.Chen,"Multicasting Streaming Media to Mobile Users", IEEE Communications Magazine,Oct,2003.p.81-89.
[3] A.Dutta,S.Das,W.Chen,A.MacAuley, "MarconiNet supporting Streaming Media over Localized Wireless Multicast",WMC'02,Sept. 2002,p.61-69.
[4] S.Deering,RFC1112:Host Extesions for IP Multicasting,IETF,Aug.1989.
[5] W.Fenner,RFC2236:Internet Group Management Protocol, Version 2, IETF,Nov.1997.
[6] B.Fenner,H.He,B.Haberman,H.Sandick, IETF Draft:IGMP/MLD-based Multicast Forwarding, IETF, Apr.2004.
[7] B.Liang,J.Haas, "Predictive Distance-Based Mobility Management for Multidimensional PCS Networks," IEEE/ACM Transactions on Networking,Vol.11,No.5,Oct.2003.
[8] C.Cho,S.Jun,E.Paik,K.Park, "Rate Control for Streaming Services Based on Mobility Prediction in Wireless Mobile Networks", in Proc.of IEEE WCNC05,Mar.2005.
[9] Legout,E.Biersack.: "PLM: fast convergency for cumulative layered multicast transmission schemes",in Proc. ACM SIGMETRICS'2000, Santa Clra,CA,USA,pp.113-22,June 2000.
[10] M.Jain,C.Dovrolis.: "End-to-end available bandwidth: measurement methodology, dynamics, and relation with TCP throughput", IEEE/ACM Trans.on Networking,Vol.1 1(4),pp.537-549,2003.
[11] M.Welzl.:Network Congestion Control managing internet traffic, Wiley, India, pg.7-15,69-77,93-96,2005.
[12] McCanne S.,Jacobson V.,and Vetterli M.:Receiver-driven layered multicast,Proceedings of ACM SIGCOMM,pp.117-130,August 1996, New York,USA.
[13] ns2:http://www.isi.edu/nsnam/ns/