
# Study on PLC with Switch Management in Intelligent Manufacturing Network

Guangfu Wang
Sichuan Electromechanical Institute of Vocation and Technology
Panzhihua, Sichuan, China
Emails: wangguangfu126@126.com

***Submitted: Jan. 16, 2014*** ***Accepted: Apr. 2, 2014*** ***Published: June 1, 2014***

***Abstract- This paper discusses a new solution for switch management in intelligent manufacturing network. It makes PLC (Programmable Logic Controller) communication module have the switch management features and exchange I/O data in manufacturing network. The switch manager has used the chip of the Ethernet switch device 88E6165. The Marvell 88E6165 device embedded in communication devices is a single-chip 6 port gigabit Ethernet switch with five integrated gigabit Ethernet transceivers. It performs the tasks of switch management, a series of services and applications are supported in PLC when it is running in a manufacturing network. It also analyzes the potential network topologies in which our customers may use the communication module and how the communication module's architecture facilitates these topologies. Actors associated with the switch management service are described further. It proposes a new mechanism to minimize the congestion based on the measure of taking an adaptive decision during transferring multicast messages to handle multicast message growing with industrial Ethernet for manufacturing systems. Proposed approach is***

***to accomplish a device requesting to start and stop the reception of the multicast streams. It joins and leaves message requests through IGMP. Final, an application prototype system contains various devices and the global architecture is proposed to provide transparency between control network and device (IO) network.***

**Index terms*:* IGMP, industrial Ethernet, manufacturing network, switch management, PLC**

## I. INTRODUCTION

The switch manager service of the intelligent manufacturing system 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 (Internet Group Management Protocol) 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 [1].

The process of a device requesting to start and stop the reception of the multicast streams is accomplished through IGMP join (A.K.A. Report message) 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 MNOC, however, does not provide this capability and requires that another device in the network supports the querier functionality [2]. 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.

In a situation where the querier device is not known, for example when the device 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 [3]. 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. 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 (XNOC, 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 suffC1nt for IGMP Snooping to know only the direction toward the querier; the identity of the querier is not important [4].

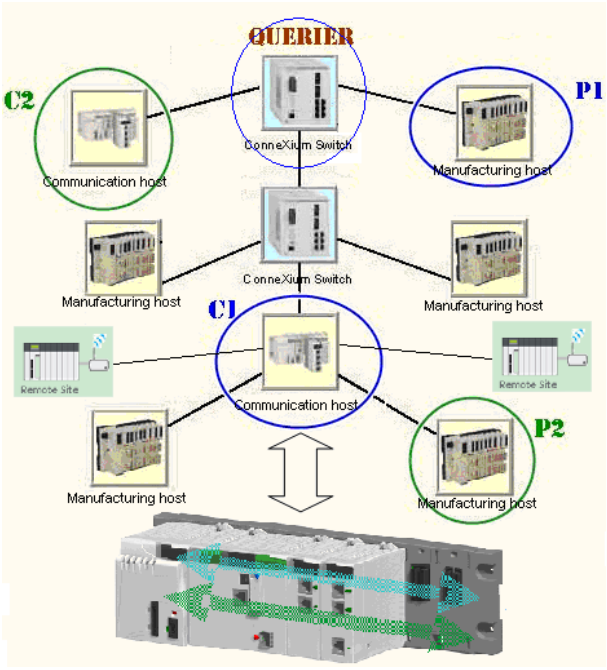


Figure 1. Example network in intelligent manufacturing system

As shown in figure 1, consider for a moment the case of a multicast producer (P1, a manufacturing host), 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, a communication host) 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. The remote site can also be connected to the querier via C1 (communication host). The communication host is the point we will study further in the next chapter. As shown in bottom part of figure 1, it is a communication example with Dual-bus backplane. One bus is for x-bus communication, which is for exchanging data with CPU for configuration data. The other bus is for e-bus communication, which is for exchanging data for Ethernet communication.

What about consuming devices (C2, a communication host) “above” the producer (P2, a manufacturing host)? 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.

In the event that a querier fails, the query messages will stop being sent into the network and the devices will stop renewing their registration for their multicast streams. The IGMP Snooping component will age out the registrations for these streams when no join messages have been seen for the specified age out time. As a result, with the loss of a querier the multicast streams will revert to being flooded in the network.

Typically multiple switches in the network will offer the querrier service. If the service is enabled on multiple switches simultaneously, the switches will negotiate for the active querier status. The switch with the lowest IP address wins. If this switch fails then other switches will notice that the querier stopped sending the query messages and each of these switches will attempt to take over the active querier role for the network. Each switch will begin sending its own query messages until it sees a query message arrive from a superior switch; a switch having a lower IP address. This negotiation can take a significant amount of time to resolve. For many

downstream devices, with all these changing query messages, the path to the new querier may be different than the previous path as the query messages are received on a different port.

For the IGMP Snooping component in our device, when it notices a querier port change it recognizes that it no longer knows where to send the multicast traffic or any join messages it receives and it begins flooding all multicast traffic. In addition, it starts a timer and if the queries continue to arrive on a particular port for a specified duration, it assumes that the querier election process has stabilized and it can then begin pruning again. During this interim period until the querier port has stabilized the IGMP Snooping component will record the join requests on each port but will continue to flood the multicast traffic. Once the querier port stabilizes it can quickly prune the multicast streams associated with the recorded joins. In the following paragraph, we will discuss the techniques and working process in details.

## II. Services Integrated in Switch

When performing the tasks of switch manager, a series of services and applications are supported in PLC when it is running in a manufacturing network.

1) Address Service

Address service includes two kinds of IP address assignment: address client and address server. FDR (Fault Device Replacement) is the address services for address assignment for the devices in manufacturing network.

FDR Client - IP parameters (IP Address, Subnet Mask, and Gateway) of this module are configurable by UnityPro/DTM software. FDR Client service is used to assign IP parameters.

The module can configure Ethernet-II frame type which is not a user configurable parameter. It can meet with different types of IP addresses, such as stored IP, BOOTP, DHCP, that module can be assigned based on state of the module.

FDRServer - This service is Customer configurable service using UnityPro/DTM. Customer can configure IP parameters for a device based on a unique name (device name) or MAC address of the device. This service also allows devices to store its configuration in its local non-volatile memory. FDR server will automatically provide correct network and device parameter (Customer configuration and application) to replacement devices without stopping Customer process. FDR Client regular is mandatory feature on replacement device in order for FDR to be fully effective.

2) EIO Scanner

For manufacturing network, the I/O data for manufacturing device are handled by EIO scanned. There are two types of devices (MODBUS and EIP based) that can be scanned using this service. This service is configured using UnityPro/DTM.

Modbus Scanner - This service allows exchanging of IO data with Modbus/TCP based devices. Service supports MODBUS function codes: 3 read, 16 write, 23 read write.

EIP Scanner - This service allows exchanging of IO data (embedded in assembly objects) with EtherNet/IP based devices.

3) IO Server

Three types of service are supported as listed below.

Modbus Server - Modbus server service allows access to local Modbus server for module diagnostics and access to CPU Modbus server. Clients such as WEB-pages, MODBUS-SCADA, MODBUS-HMI, UnityPro use this service.

EIP Adapter - This service allows access to local slaves for PLC IO data, and access to local diagnostic data via CIP diagnostic objects. Clients such as WEB-pages, EIP-SCADA, EIP-HMI, DTM use this service.

EIP Modbus Translator - This service allows an EtherNet/IP client to access Modbus data without any special implementation.

4) Redundancy service

RSTP service is configurable by UnityPro. Redundancy service provides customer with full, fast, and reliable protection against single point of failure in network. This service also prevents network storm. Protocol driving this service is RSTP. Since RSTP is standard protocol defined by IEEE its choice as redundancy protocol enables customer to reliably extend networks with third party devices or include this device in preexisting network that supports RSTP without compromising network integrity.

RSTP service configuration allows user to tailor its performance and deployment to its network strategies e.g. daisy chain loop.

5) Diagnostics

There are various ways customer can diagnose the devices when using a PLC with switch management function in manufacturing network:

Diagnostics via PLC Application: Certain module diagnostics (IO connection health, Redundancy status etc) are available to PLC application and are updated every CPU cycle.

Diagnostics via Local Modbus Server: Certain module diagnostics (IO connection extended health, Redundancy status, FDR Server etc) are available to Modbus Clients by reading this area using MODBUS FC3 and Unit ID set to 255 or via MODBUS FC 8/21-22, FC 43/14.

Diagnostics via CIP Objects: Certain module diagnostics (Message Router, Redundancy, EIP Scanner etc) are available via CIP objects that EtherNet/IP devices such as SCADA or HMI can read.

Diagnostics via SNMP: Certain module diagnostics (IO connection health, Modbus Server connection list, IP parameters, Redundancy, etc) are available via SNMP service.

Diagnostics of Ethernet Ports: You can diagnose network issues by examining packets coming in & out of Ethernet ports by using Port Mirroring feature supported by this module which is explained later.

Diagnostics via embedded Web pages: Embedded web pages will provide diagnostics data by sending Modbus or EtherNet/IP requests to the module.

6) SNMP service

This service is Customer configurable service via UnityPro software. This service allows customer easy access to modules diagnostic information as well as event notification for certain services (ex. network topology change) via widely used SNMP protocol. Customer is able to configure SNMP manager IP addresses (MIB browser, CNM etc) as trap (event) notification destinations. Diagnostic information provided by SNMP service can be summarized as: Standard MIB 2, TCP/IP diagnostic, Bridge MIB, Private MIB, Port 502 Messaging, IOScanner diagnostic, Switch diagnostic, etc.

## III. Network Topology for Communication Host

This section simply analyzes the potential network topologies in which our customers may use the C1 module and how the C1 module's architecture facilitates these topologies.

a. Simple Network Topology

Figure 2 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 C1 module involves. All the C1 modules can be used in this topology network [5].

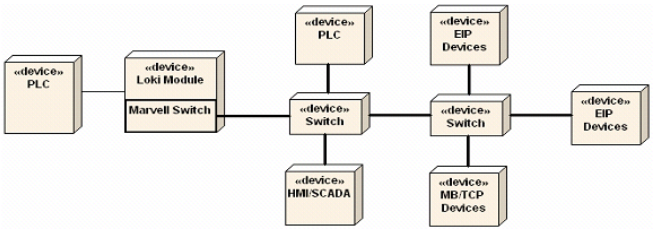


Figure 2. The simple network topology of the C1 control network

Because of no loop in the simple network topology, the RSTP functionality can be disabled to save the bandwidths of the C1 CPU and the network and reduce network traffics. Therefore, this version of the C1 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].

In the simple network topology, the C1 modules as the communication modules for their corresponding PLCs can only be used as end devices; the C1 module can act as an end device and/or a switch as shown in Figure 3.

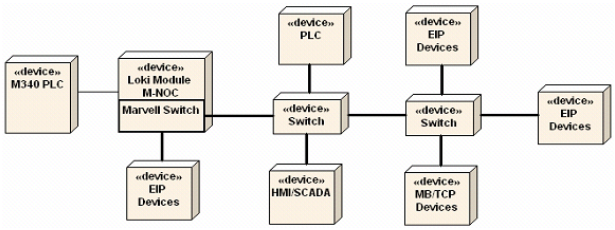


Figure 3. The simple network topology with the C1 module

b. Switch Ring Topology

Figure 4 shows a simple switch ring network topology in which the C1 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].

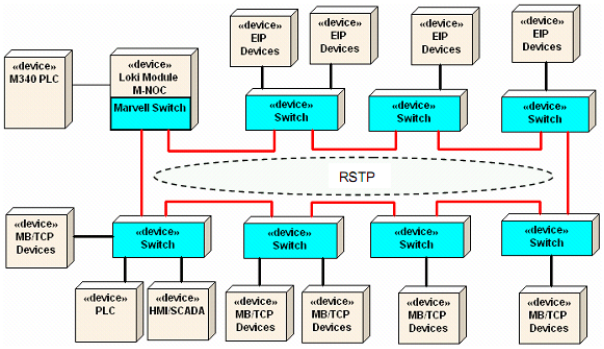


Figure 4. The switch ring network topology with the C1 module

In this topology, the fault recover time is mainly determined by the network infrastructure switches the users choose, not mainly by the C1 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 C1 module can be used by the user to connect to the switch ring, this version of the C1 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.

## IV. User Cases of Switch Manager

The switch manager has used the chip of the Ethernet switch device 88E6165. The Marvell 88E6165 device embedded in communication devices is a single-chip 6 port gigabit Ethernet switch with five integrated gigabit Ethernet transceivers. Configuration of the switch involves standard setting of port properties, i.e. port speed and duplex. If the port is enabled with RSTP service, which is a loop-prevention protocol or algorithm, it heavily relies on this device to run in

the controller. Other services that rely on switch features include QOS, IGMP snooping, and port mirroring [9]. To support these protocols and features, this device provides the following special features:

(1) Support of the Marvell DSA (Distributed Switching Architecture) for RSTP, IGMP and CPU-directed packet processing.

(2) Port states & management frame handling for RSTP and IGMP Snooping.

(3) Prioritization queues for QoS (Quality of Service).

(4) Port mirroring diagnostics for port mirroring.

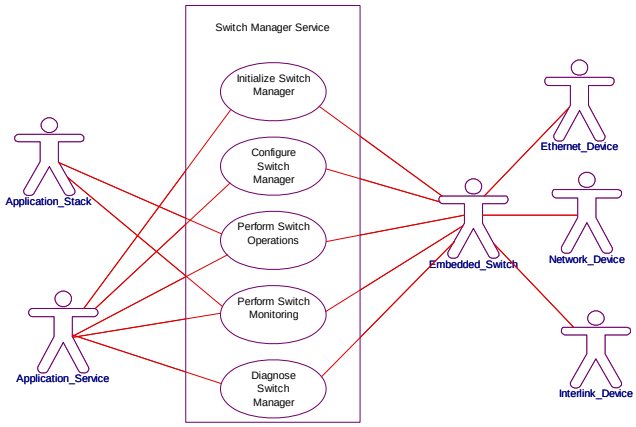


Figure 5. Use case(s)

The switch manager can be presented from two different viewpoints: the use cases and the configuration. The use cases describe the service from the point of view of the actors that interact with it. The configuration provides an external view of the service and the environment in which it is intended to operate.

Figure 5 provides the reader with a customer view of the service being specified. Actors and their interaction with the service are defined here. This provides the highest level view of the service architecture.

## V. Actors and Process

Actors associated with the Switch Manager Service are described as follows:

Application Service: an application service is any service in a CCS platform device which requires the switch manager features. RSTP Service: an application service that interacts with this

service to provide cable redundancy. IGMP Service: an application service that interacts with this service to manage IP group messaging. Application Stack: an application service is any service in a CCS platform device which requires the QoS information. Embedded Switch: a hardware component allows that provides connectivity to target devices over a network using multiple ports. Engineering tool: allow users to perform configuration, operation, maintenance and diagnostics. Network Device: an Ethernet Device is used to interact with on the device network such as the Ethernet CRA module. The Dual-Ring Switch: Switch is used to connect a redundant CRP module, general Ethernet switches and general Distributed IO modules. Ethernet Device: An Ethernet devices that attach to the service port of a CCS Step one module, such as a Customer Engineering Tool, or a NOC-DIO module in extended mode [10].

The relationship and interaction of these actors with the switch manager service is described process in the following:.

a. Initialize Switch Manager

Initializing switch manager describes the initialization of the switch manager and the embedded switch.

The initialization of switch manager behavior is as follows:

If the host module is in factory mode the switch manager service will initialize the embedded switch and switch manager service as defined by the factory default behavior. If the host module is not in factory mode the switch manager service will initialize the embedded switch and switch manager service as defined by the default behavior.

b. Configure Switch Manager

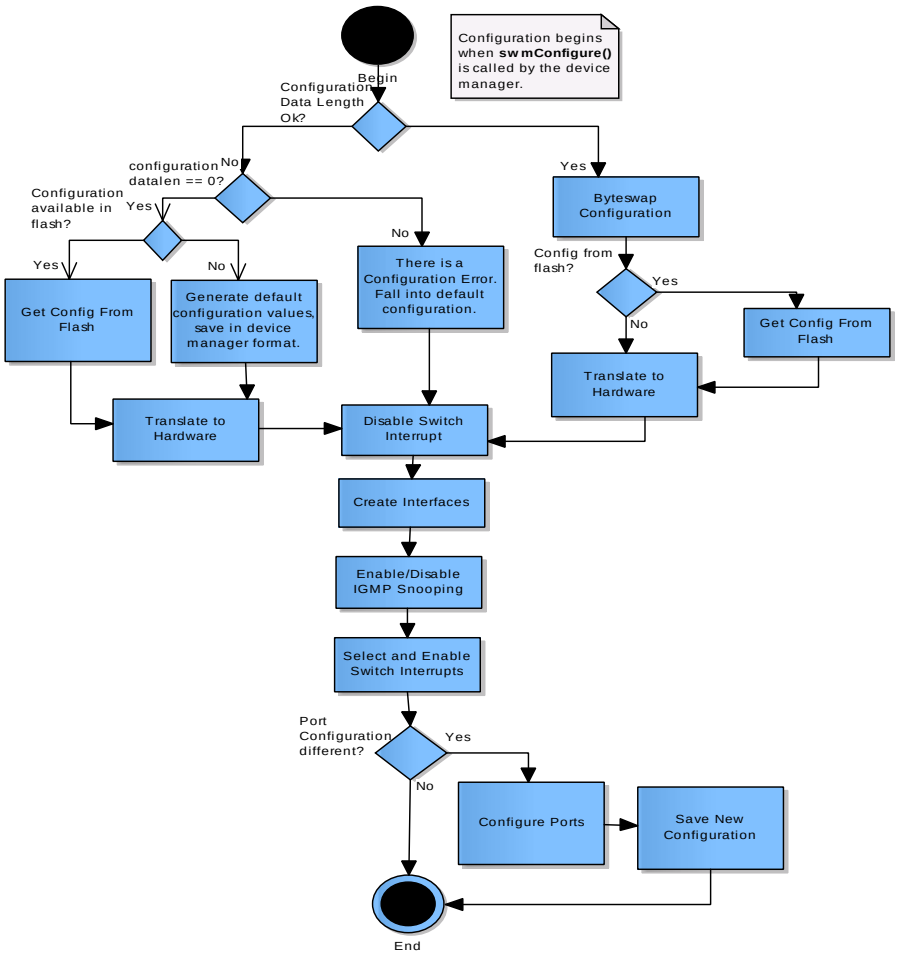


Figure 6. Switch manager configuration flow chart

Configuring switch manager use case describes the configuration of the switch manage and the embedded switch by any application service while the host module and embedded switch are operational.

The switch manager service allows an application service to configure switch manager and the embedded switch. The configure switch manager behavior is as follows: As shown in figure 6, configuring is called whenever there is a new configuration made available to the device manager. This may happen for a variety of reasons such as user download of new configuration, link down/link up events, etc. However, the switch manager configuration may not change between calls to configuration and it is best not to perturb the network by trying to change port states if there is no need to. Therefore the configuration is always compared to a stored version of the configuration before any actions take place. If the configuration has changed, then the same

approach is take on a per port basis and ports with identical configurations between versions are not modified. Configuration also creates or destroys interfaces if the services they are associated with are required in the new configuration or disabled. The configuration may be stored in flash memory or it may be passed to it by the device manager. The configuration is always stored in logical format meaning port 0 is the internal port, port 1 is the first external port, etc and must be translated to match the correct hardware's physical port layout before configuring the switch. The configuration given to the switch manager is with bit 0 being the least significant bit [11].

c. Emit RSTP Configuration Messages

The RSTP protocol requires the switch to send configuration message periodically to advertise its current understanding of the spanning tree topology and its own state. The constant emitting of the configuration message is controlled by a timer called hello timer. The timeout value of the hello timer is from 1 to 10 seconds with 2 second as its default. The timeout value of the hello timer should be configurable by the users to balance the effC1ncy of detecting the topology changes and the network traffic based on their production environment. If the timeout is larger, it will result in a slower detection of failure. But if it is smaller, it will increase the network traffic load and more CPU bandwidth for RSTP processing [12].

d. Calculate and Maintain the Spanning Tree

Upon running normally, the switch always listens to the configuration messages from the other switches.

Once receiving a configuration message, the switch with RSTP compares the advertised information to its own internal information (mostly switch MAC, switch priority, port MAC, port priority, and path cost) to determine root bridge, root port, designated bridge, designated port, and so on, maintain a unique path to root and a unique path to other designated switch, and update its own information [13]. When the switch finds out that the optimum spanning tree is different from currently active set, it takes actions to initialize the topology change appropriately.

e. Initialize Topology Change

Once determining a topology change needed (that is, non-edge ports moving to the forwarding state), the RSTP component sends topology change messages through the non-edge ports [14].

## VI. IGMP Management and its Process

a. Requirement of Industrial Ethernet

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 [15]. 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. 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 [16]. 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.

b. IGMP Snooping Service

The IGMP Snooping service of our product (Intelligent Controller for Industrial Ethernet, C1) 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 [17]. 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.

c. 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 [18]. The C1, 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.

In a situation where the querier device is not known, for example when the C1 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 [19], 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 [20]. 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 (C1, 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 suffC1nt for IGMP Snooping to know only the direction toward the querier; the identity of the querier is not important [21].

In the event that a querier fails, the query messages will stop being sent into the network and the devices will stop renewing their registration for their multicast streams. The IGMP Snooping component will age out the registrations for these streams when no join messages have been seen for the specified age out time. As a result, with the loss of a querier the multicast streams will revert to being flooded in the network [22].

## VII. IGMP Implementation

a. Functionality Design

The Switch Management subsystem functionalities are mapped to two tasks in the system. The RSTP task executes the functionalities of managing the switch, receiving and processing RSTP messages, emitting RSTP Configuration messages, calculating and maintaining the spanning tree, and initializing the topology change. The IGMP Snooping task performs the IGMP Snooping operation functionality. The Switch Management component operations (initialization, configuration, start, and so on) and its diagnostic data accessing functionality are executed in the Ethernet Manager task context. The IGMP Snooping component interacts with the Switch Manager directly and with the Ethernet Manager and the RSTP component indirectly through the Switch Manager. The Switch Manager gets its configuration information from the Ethernet Manager and from that determines if IGMP Snooping is to be enabled, disabled or reset. IGMP Snooping then interacts with the Switch Manager to register / deregister with the VxWorks stack for reception and transmission of the IGMP traffic [23].

The IGMP Snooping component links to the VxWorks stack via a “snarfing protocol” to allow it to grab copies of inbound and outbound IGMP packets. The IGMP Snoop Component snarfs Marvell Link Street MV88E61xx DSA-tagged IGMP traffic to intellegently route multicast traffic on the switch ports of the MV88E61xx. Although this library uses the VxWorks protocol layer API to capture incoming and outgoing network traffic, it is not generic enough to provide IGMP switch snooping functionality on a generic multi-interface target [24].

b. Interaction of Components

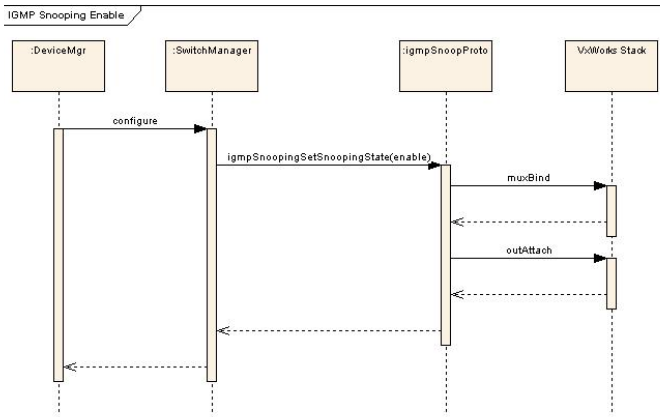


Figure 7. Enable action of IGMP snooping

The switch passes IGMP traffic from the external switch ports to the CPU for snooping and forwarding via the CPU Ethernet interface. These packets differ from normal Ethernet packets in that an 8-byte “Ethernet type DSA tag” is injected into the packet between the Ethernet source address and the Ethernet type field. An IGMP packet received by the MUX_PROTO_SNARF receive routine (igmpSnoopReceive()) is snooped and possibly forwarded to a subset of the external ports and/or allowed up the IP stack [25].

IGMP packets coming down from the IP stack are captured by the MUX_PROTO_OUTPUT receive routine (igmpSnoopOutReceive()), injected with an Ethernet type DSA tag, and processed by the MUX_PROTO_SNARF receive routine (igmpSnooopReceive()) via a direct call. This additional lash-up is necessary because the switch excludes the CPU port from the IGMP snoop signaling. Figure 7 and figure 8 are the sequence diagrams of enable action and disable action.

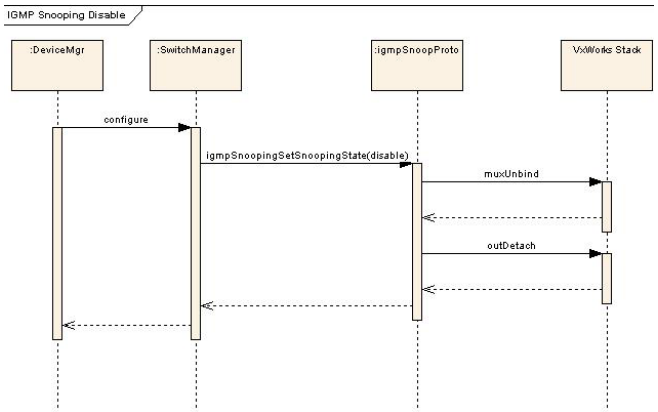


Figure 8. Disable action of IGMP snooping

c. API of Components

The Switch Manager calls into this library via four function calls. These calls are documented fully within this module and are summarized below:

igmpSnoopingNotifyLinkState() - signal a link state change. igmpSnoopingTopologyChangeNotice() - signal an RSTP-detected change. igmpSnoopingSetSnoopingState() - bind/unbind/reset the IGMP Snoop Component. igmpSnoopingSetSnoopingGet() - return state of IGMP Snoop Component. The IGMP Snoop Component consists of three functional units:

c.i Protocol Layer

The protocol layer, which consists mainly of igmpSnoopReceive() and igmpSnoopOutReceive(), is responsible for watching packets as they enter and leave the Ethernet interface of the CPU. Most packets are ingored and passed on, but IGMP packets are processed. An IGMP packet can be read to extract information about the Querier, to add groups and/or ports to the internal group database, and enhance the multicast forwarding of the switch. IGMP packets are typically only forwarded to ports with the “need to know” [26].

c.ii Task

The igmpSnoopTask() routine is used to periodically wake up and evaluate whether the state of the Querier needs to be changed, or if the internal group database should be reduced. Changes to the state of the Querier can cause the switch to be multicast-forwarding-engaged, or to flood multicast traffic. Groups/ports in the internal group database are checked for age and are potentially pruned. Such a pruning event is communicated to the switch if the switch is engaged [27].

c.iii Control and Event Notification API

The Control and Event Notification API is used by the Switch Manager to bind, unbind and reset (erase the internal group database and flood) the IGMP Snoop Component. It is also used to notify the IGMP Snoop Component of port link status, and RSTP-detected changes.

c.iiii Querier State

The IGMP Snoop Component must maintain a state of the Querier and remembers the port it is on. The states of the Querier are IGMP_SNOOP_QUERIER_NONE, or “NONE” when a Querier is not detected; IGMP_SNOOP_QUERIER_NEW, or “NEW” when a Querier has been detected but has not been around long enough to engage the switch to intelligently forward (and not flood) multicast; and IGMP_SNOOP_QUERIER_ESTABLISHED, or “ESTABLISHED” when the Querier has been active long enough to engage multicast forwarding in the switch [28]. The

switch is set by the IGMP Snoop Component to flood multicast in the NONE and NEW states, and to forward in the ESTABLISHED state. The NEW state is used by the IGMP Snoop Component to gain confidence in the Querier and learn the whereabouts of the group subscribers [29].

The IGMP Snoop Component has two states: SNOOPING_ENABLED and SNOOPING_DISABLED. When the IGMP Snoop Component is ENABLED, the IGMP Snoop Component task is started, the protocol layer is bound to the MUX, and the Querier state is set to IGMP_SNOOP_QUERIER_NONE. When the IGMP Snoop Component is DISABLED, the switch is set to flood, the IGMP Snoop Component task is deleted, and the protocol layer is unbound from the MUX. Figure 9 is the querier state of IGMP snooping [30].

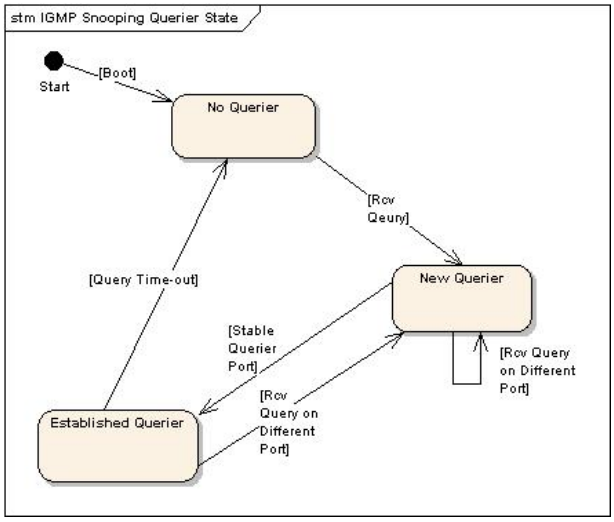


Figure 9. Querier state

## VIII. Application in Manufacturing Network

The prototype system contains various devices and the global architecture diagram is as shown in figure 10. The system is to provide transparency between Control Network and Device (IO) network, provide Remote IO functionality on Ethernet using EIP protocol (functionality similar to S908 RIO system) which guarantees determinism, allow RIO devices and DIO devices to co-exist(s) in Device (IO) network without affecting determinism, support Hot-Standby functionality on Ethernet and all services and allow Ethernet gateway device(s) such as Profibus Master, CANopen Master to operate as DIO device.

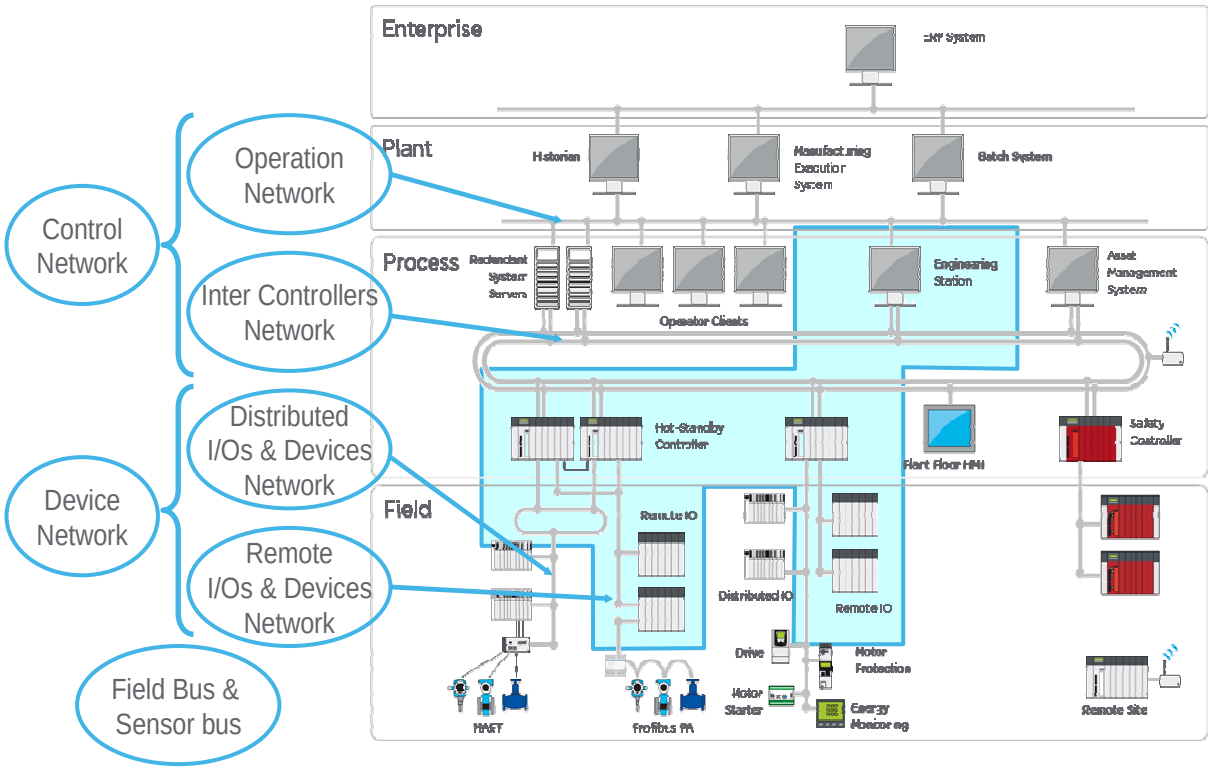


Figure 10. System Architecture

It is working based on the switched network [31]. The architecture is designed and tested for simultaneous use of industrial Ethernet and control system in manufacturing network. In the system architecture deployment, the related devices include: Quantum PSx CPU, Quantum CRP module, Quantum NOC-DIO module, Quantum NOC-CTRL module, Quantum CRA and M340 BMX CRA. The architecture we used includes Ethernet local rack, Ethernet remote I/O drops, Ethernet distributed I/O devices, ConneXium extended managed switches, preconfigured to serve as dual-ring switches (DRSs), hot standby configuration, remote I/O and distributed I/O devices (integrated on the same physical network), third-party devices (distributed I/O devices), daisy-chain loop architectures provided by DRSs and communication modules with dual Ethernet ports. It also called Ethernet IO system. The typical application of it is Q-series EIO system. The Q-series EIO system provides automatic network recovery of less than 50 ms and deterministic remote I/O performance. A Q-series EIO system uses the same Q-series I/O modules as a Q-series legacy remote I/O system (S908).

## IX. Conclusions and Perspective

This paper has givens a new solution for switch management in intelligent manufacturing network. It makes PLC communication module have the switch management features and exchange I/O data in manufacturing network. The new intelligent communication module performs the tasks of switch management, a series of services and applications are supported in PLC when it is running in a manufacturing network. It analyzed the potential network topologies in which our customers may use the communication module and how the communication module's architecture facilitates these topologies. Actors associated with the switch management service were described further. And we proposed a new solution to do management for multicast message in industrial area with IGMP Snooping method which is based on the taking an adaptive decision during transferring multicast messages. The whole system architecture is to provide transparency between Control Network and Device (IO) network, provide Remote IO functionality on Ethernet using EIP protocol which guarantees determinism, allow RIO devices and DIO devices to co-exist(s) in Device (IO) network without affecting determinism, support Hot-Standby functionality on Ethernet and all services and allow Ethernet gateway device(s) such as Profibus Master, CANopen Master to operate as DIO device. It is a now solution to build intelligent manufacturing network.

## REFERENCES

[1] Xie, Pengshou and Rui, Zhiyuan. Study on the integration framework and reliable information transmission of manufacturing integrated services platform, Journal of Computers (Finland), v 8, n 1, p 146-154, 2013

[2] Kwon,G.I. and Byers,J.: Smooth multirate multicast congestion control, Proceedings of IEEE Infocom, vol.2, pp.1022-1032, March 2003.

[3] ETRI, TTA, "Specifications for 2.3 GHz band Portable Internet Service", Apr. 2004.

[4] A.Dutta, J.Chennikara, W.Chen, "Multicasting Streaming Media to Mobile Users", IEEE Communications Magazine, Oct,2003. p.81-89.

[5] A.Dutta, S.Das,W.Chen, A.MacAuley, "MarconiNet supporting Streaming Media over Localized Wireless Multicast", WMC'02, Sept. 2002, p.61-69.

[6] S.Deering, RFC1112:Host Extesions for IP Multicasting, IETF, Aug.1989.

[7] W.Fenner, RFC2236: Internet Group Management Protocol, Version 2, IETF, Nov. 1997.

[8] B.Fenner, H.He, B.Haberman, H.Sandick, IETF Draft: IGMP/MLD-based Multicast Forwarding, IETF, Apr. 2004.

[9] B.Liang, J.Haas, “Predictive Distance-Based Mobility Management for Multidimensional PCS Networks,” IEEE/ACM Transactions on Networking, Vol. 11, No.5, Oct. 2003.

[10] 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.

[11] 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.

[12] 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.

[13] M.Welzl.: Network Congestion Control managing internet traffic, Wiley, India, pg.7-15, 69-77, 93-96, 2005.

[14] McCanne S., Jacobson V., and Vetterli M.: Receiver-driven layered multicast, Proceedings of ACM SIGCOMM, pp.117-130, August 1996, New York, USA.

[15] ns2: http://www.isi.edu/nsnam/ns/

[16] Postel,J.: Internet protocol, Request for Comments 791, September, 1981.

[17] Qian Zhang, Quji Guo, Qiang Ni, Wenwu Zhu, and Ya-Qin Zhang.: Source adaptive multi-layered multicast algorithms for realtime video distribution, IEEE/ACM Transactions on Networking, vol.8, no.6. pp.720-733, 2006.

[18] S.McCanne, M.Vetterli, and V.Jacobson.: Low-complexity video coding for receiver driven layered multicast, IEEE Journal on Selected Areas in Communications, vol.15, no.6, pg.982-1001, 1997.

[19] Satish Kumar, Pavlin Radoslavov, David Thaler, Cengiz Alaettinoglu, Deborah Estrin, Mark Handley.: The MASCBGMP Architecture for Inter-domain Multicast Routing,in ACM SIGCOMM, April 1998, pp. 93 to 104.

[20] Stian Johansen, Anna N.Kim, Andrew Perkis.: “Quality Incentive Assisted Congestion Control for Receiver-Driven Multicast” IEEE Communications Society ICC 2007.

[21] Deering.S.: Multicasting Routing in Internetwork and Extended LANs, SIGCOMM Summer 1988 Proceeding, Aug 1988.

[22] Distance Vector Multicast Routing Protocol, Request for Comments 1075, November 1988.

[23] J.Byers, M.Frumin, et al., "FLID-DL: congestion control for layered multicast", in Proc. NGC2000, Palo Alto, USA, pp.71-81, Nov.2000.

[24] J.C.Bennett, H.Zhang.: "Hierarchical packet fair queuing algorithms", IEEE/ACM Trans. on Networking, Vol.5(5), pp.675-689, 1997.

[25] Xylomenos, George; Katsaros, Konstantinos; Tsakanikas, Vasilis. Support of multiple content variants in the multimedia broadcast/multicast service, Volume 24, International Journal of Communication Systems, Pages 1175, June 2011.

[26] Tan, Yee Chieh; Ramli, Nordin Bin; Chuah, Teong Chee. Time-domain equalizer for multicarrier systems in impulsive noise. Volume 25, International Journal of Communication Systems, Pages 1256, Feb. 2012.

[27] Liu, Wei; Jin, Huan; Wang, Xinbing; Guizani, Mohsen. A novel IEEE 802.11-based MAC protocol supporting cooperative communications. Volume 24, International Journal of Communication Systems, Pages 1235, Nov. 2011

[28] Wu, Shaoen; Biaz, Saad; Wang, Honggang. Rate adaptation with loss diagnosis on IEEE 802.11 networks, Volume 25, International Journal of Communication Systems, Pages 1276, Apr.2012

[29] Wang, Jingyang; Huang, Min; Wang, Haiyao; Guo, Liwei; Zhou, Wanzhen. Research on detectable and indicative forward active network congestion control algorithm. Journal of Software (Finland), v 7, n 6, p 1195-1202, 2012

[30] Pang, Qingle. Information fusion based fault location technology for distribution network. Journal of Software (Finland), v 6, n 5, p 826-833, 2011

[31] Hu, Wenmin; Lu, Zhonghai; Liu, Hengzhu; Jantsch, Axel. TPSS: A flexible hardware support for unicast and multicast on networks-on-chip. Journal of Computers (Finland), v 7, n 7, p 1743-1752, 2012