Automatic device configuration for Ethernet ring redundancy protocols

Oliver Kleineberg, Michael Ries, Markus Rentschler
Hirschmann Automation & Control GmbH
Stuttgarter Straße 45-51
DE-72654 Neckartenzlingen
{oliver.kleineberg, michael.ries, markus.rentschler}@hirschmann.de

Max Felser
Bern University of Applied Science
Engineering and Information Technology
Jlcoweg 1, CH-3400 Burgdorf
max.felser@bfh.ch

Abstract

In modern communication systems based on Ethernet technology, the use of physical ring structures and ring redundancy protocols has been common for some time in the past. A challenge remains the configuration of such a redundancy protocol on each device with the networks stretching out over large areas, like in offshore wind power stations, where each windmill houses at least one Ethernet switch. The distance between windmills can be several kilometers and configuration of the redundancy protocol on each device is an elaborate process. In this paper, a mechanism is proposed which automatizes the configuration of ring redundancy protocols and eliminates the need to configure each device separately. The actual protocol implementation is intended to be part of the next major software release of Hirschmann Industrial Ethernet Switches.

1. Introduction and Motivation

Ethernet technology has become an essential part of many modern communication infrastructures. In the past years, it has been very successful in the field of industrial automation systems. Recently, with further technological advancement concerning reliability and performance, Ethernet technology is transpiring further and further into new application domains like power utility automation in case of the IEC 61850, or train and transportation systems. This trend is continuously advancing; the technology is far from its limits. Ethernet is claiming more and more application fields, and where in the past, Ethernet installations where limited to network systems with small physical diameters and low numbers of devices, modern applications more and more pose the need for distributed communication systems over large areas with an increasing number of network devices.

More and more, Ethernet based systems are also used in mission critical applications. So the availability of the network is getting more and more a critical issue. In [1] different requirements are outlined and in [2] different methods for high available media systems are evaluated. In [3] these different solutions are specified.

Distribution of communication networks also means the distribution of technical devices, these communication networks are based on, over large areas. Therefore, now and even to a greater degree in the future, Ethernet switches will be distributed over large areas, out of the immediate physical reach e.g. from service personnel or network engineers, with a substantial increase in device numbers.

Another major challenge for Ethernet adoption in new application fields is not a technical aspect, but a socio-technical one: a specialist in an application field, where Ethernet is considered to be a future means of communication, potentially replacing non-standardized, proprietary cabling and protocols, has to understand and to handle what he or she is working with. He or she may not be or even cannot be an Ethernet specialist, but must be able to work with the technology and Ethernet must not deviate him or her from the actual work, consuming valuable time and resources. A power protection systems electrical engineer wishes not and should not be forced to configure Ethernet switches elaborately for power utility communication systems to work.

Different protocols are developed to support the installation and planning of such Ethernet installations and give more and more practical value as shown in [4] and [5].

A protocol, which is able to configure ring redundancy protocols on Ethernet switches automatically, therefore is of great use: Network engineers can configure a large number of devices already in the field, potentially distributed over a large area, while people dependant on Ethernet technology as communication infrastructure can be presented with a solution that allows them to configure a redundant network with little effort. The general idea how to automatically configure ring network devices has been given in [6] with the actual detailed implementation left open.

A challenge to the actual implementation is the ability for the protocol to detect additional physical loop structures that are present in addition to the ring that needs to be configured. The protocol implementation not only needs to configure devices, but also needs to detect and report these loops so that the configuration on the intended physical ring can be made.

2. Ethernet Ring Networks and Protocols

The physical ring structure is well suited for a distributed network application, as it allows different participants in communication systems to be allocated over a large physical diameter with low cabling effort, compared to other physical topologies like star or tree topologies. Instead of connecting each participant to a central distribution device and creating a star network, all participants are interlinked, with the last device in the list connecting to the first device, closing the ring.

2.1. Ring redundancy protocol example

There are several ring redundancy protocols in existence and used on the market, like the Siemens OSM ring, the Hirschmann HiPER Ring and many other protocols from other manufacturers. The Media Redundancy Protocol (MRP) however, has been included in the international standard IEC 62439 – High availability automation networks. The proposed mechanisms in this paper can be implemented in e.g. a network switch software amongst other for the MRP protocol, but the mechanism is not limited to MRP, but to all ring redundancy protocols that operate after similar mode of operation.

The MRP works with a dedicated master – client structure, where a ring is compromised of one master node called the Media Redundancy Master (MRM) and several client nodes called Media Redundancy Clients (MRC). In order to break the physical loop introduced by the physical ring structure on the logical level, the MRM sets one of its ring ports into blocking mode, only receiving and transmitting MRPDUs (Media Redundancy Protocol Data Units) on this interface. Normal user traffic is not relayed on the blocked port, only on the second ring port, which remains in forwarding state. This translates the ring structure to a line structure without loops on the logical level.

For redundancy surveillance, the MRM transmits MRP test frames from both its ring ports. These test frames are sent to a specified MAC (Media Access Control) multicast address which allows a switch to identify PDUs for this protocol on the basis of the MAC address and to handle the messages accordingly. By default if no means of manipulation of any kind are implemented on the switches, frames sent to a MAC multicast address are handled like frames sent to a MAC broadcast address: They are forwarded to every network port except the port they were received at.

The test frames will be received and identified by the MRCs on one ring port and subsequently only be transmitted on the corresponding other ring port. Each test frame sent by the MRM on one ring port will eventually be received by the MRM on the corresponding other ring port. Reception of test frames on both ring ports signals the Media Redundancy Master that the network is in good health. As soon as a fault occurs in the ring network, the MRP test frames will stop being transmitted over the whole ring and subsequently, the MRM will stop receiving its sent test frames. Additionally, an MRC can inform the MRM about changes in the topology via link change frames. This signals the MRM that the ring network is broken at one point in the topology and that the MRM needs to open its formerly blocked network port for user traffic.

As soon as the network error is repaired, the MRM will again receive its MRP test frames and will again block one ring port.

2.2. MRP and Profinet IO

Profinet is an automation network, based on and compatible to Ethernet (IEEE 802.3) and specified in IEC 61158-5-10 [7] and IEC 61158-6-10 [8] and IEC 61784-2 [9]. A Profinet IO-system consists of an IO-controller, one or more IO-devices and possible IO-supervisors. The IO-supervisors are typically engineering tools. In a typical Profinet IO-system an IO-controller does control one or more IO-devices. Reference [10] provides a good overview about the functions of Profinet.

The specification provides three conformance classes of Profinet IO-systems. These classes differ in the supported application-, communication- and redundancy-classes and specify the required features. Higher classes are compatible to the lower ones.

Class A specifies certified IO-controllers and IO-devices with standard Ethernet interfaces and standard Ethernet network infrastructure. Class B requires in addition to Class A that the network infrastructure conforms to the Profinet specification. Media Redundancy Protocol (MRP) is required to support Class B and thus basic redundancy network structures are possible. Additional redundancy protocols are optional. In class C Profinet IO-systems, additionally to the MRP also the Media Redundancy Real-Time (MRRT) protocol and the Isochronous Realtime (IRT) protocols are mandatory.

With the MRP being an integral part of the Profinet redundancy concept, the proposed automatic ring configuration protocol can also be used to configure Profinet redundant ring structures. With Conformance Class B, in addition to MRP, the use of LLDP (Link Layer Discovery Protocol) is mandatory. This further adds to the usefulness in regards to device and capability detection of the protocol in Profinet environments, as described later in this paper in 3.6.

3. Automatic device configuration

The basic fact why an automatic configuration of ring devices is possible at all is that each ring node in a fully functional redundant ring network has exactly two distinguished network ports that are part of the ring. These ports are identifiable and configurable e.g. through a switches' web configuration interface or a command line interface via serial link or telnet.

A complete detection and configuration cycle from a user's point of view would be a detection initiation via user command on the MRM and after successful ring detection, which means that no additional loops were detected, a subsequent configuration initiation via a second user command. A one step solution cannot be done, because as mentioned, before the configuration takes place, it has to be certain that the ring which is intended to be configured is the only loop structure in the network.

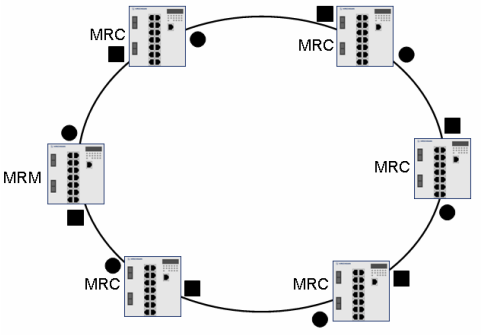

figure 1. example ring network

Figure 1 shows a ring network consisting only of switch nodes. The two ring ports on each device are marked with a circle and a square. Without any further interpretation, this network can be viewed as a simple, undirected regular graph. When the functionality of MRP test frames is applied to this network, this changes the view of the network paths. From the MRM, test frames egress both the circle and the square port. The graph representing the network has exactly one link between every two vertices, in this case represented by network switches, and the frame will, unless the network has been damaged, ingress the adjacent device on a ring port. This means that, for a specific MRP test frame from a port of the MRM, the ring represents itself as a directed graph. In figure 2, it is shown that a frame traveling clockwise from the MRM always egresses a network port marked with a circle while counter-clockwise, a frame always egresses a port marked with a square. In this basic, trivial topology, a frame will travel exactly the path the ring has to be configured. It will pass both ring ports on all devices in the ring, even if the devices are not already configured as participants in a redundant ring network. So the basic idea is, that special configuration PDUs, sent out from the MRM in a manner similar to the MRP test frames, will be used to propagate configuration information to all devices in a ring network and to test the network structure against additional loops.

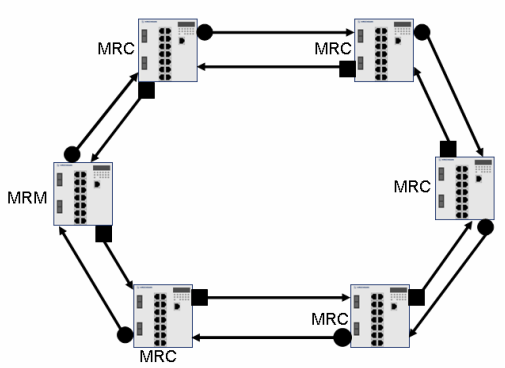

figure 2. Interpretation as directed graph

The ingress and egress ports of these configuration PDUs (one from each direction in the network) mark the ring ports, the device has to be configured with.

These configuration PDUs include in their SDU (Service Data Unit) all relevant parameters for the ring redundancy protocol that need to be configured on the individual switches. In the case of MRP, this includes e.g. the timing constraints, defined by the protocols' consistent set of parameters, and a ring VLAN ID (Virtual Local Area Network Identifier). In addition, it also includes a hop count which indicates how many devices the individual PDU has passed and which is incremented in every device upon reception, a sequence number, which is incremented in the sending MRM for each set of PDUs, one PDU for each direction, and an MRM port indicator, which identifies the original egress port of the PDU on the MRM. The port indicators are representations of the already mentioned circle and square port identifiers.

3.1. Supported topologies and challenges

When the simple ring topology is extended, it becomes clear that the characteristic of the configuration frames, sent to a MAC multicast address, will introduce some additional challenges.

Figure 3 shows the previous ring topology with MRC 1 also being the root element of an additional tree, emerging from the original ring. In this case, an additional switch structure is plugged into a non-ring port of the ring switch MRC 1. If we now consider the ring to be not configured with exception of the MRM, and the MRM starts sending configuration frames from its ring ports, these frames will eventually reach MRC 1. Now, the ports which will be configured as ring ports are not predetermined, and MRC 1 will receive the configuration frame from the "circle" direction on one

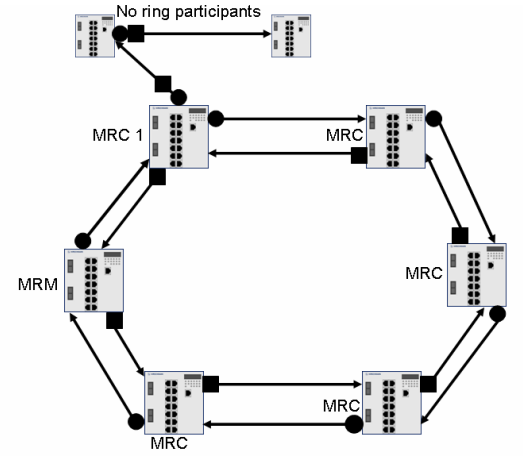

figure 3. ring with additional tree

port and forward it on all other connected ports except the receiving port. This means that with the ingress from "circle" direction, one ring port can be precisely determined, while with egress in "circle" direction, two possible ring ports are determined. With the configuration frames in "square" direction, MRC 1 can also identify its second ring port without a doubt through ingress of the frame from the "square" direction, but egress of the "square" frames takes place on all other ports of the device. This means that the non ring participant receives both configuration frames from the circle and the square port of the MRM on one interface, but as it has not received configuration frames on a second port, it can identify that it is not part of the ring structure, but part of a leaf link or tree, emerging from the original ring.

But as soon as trees emerging from the ring are meshes and contain loops themselves or the network structure is more complicated, e.g. a ring with additional links between the ring devices, the complexity rises again.

3.2. Meshed network structures

Figure 4 shows a ring structure with an additional mesh, connecting the ring nodes MRC 1 and MRC 2. When the configuration frames travel through the ring, at MRC 1, the "circle" frame will be forwarded to both mesh links: On the one hand on the link which directly connects MRC 1 and MRC 2, and on the other hand on the link to the mesh containing the "non ring participants". The configuration frames over both meshes will eventually ingress MRC 2, which without further information, cannot ascertain which port he received the configuration frame on will be the future ring port. The only parameter that distinguishes the two frames is the hop count, as two corresponding frames always carry the same sequence number and port identifer, because the frame has been duplicated at MRC 1. The same problem applies to the "square" frame, which is being duplicated at MRC 2 and will ingress MRC 1 on two different ports.

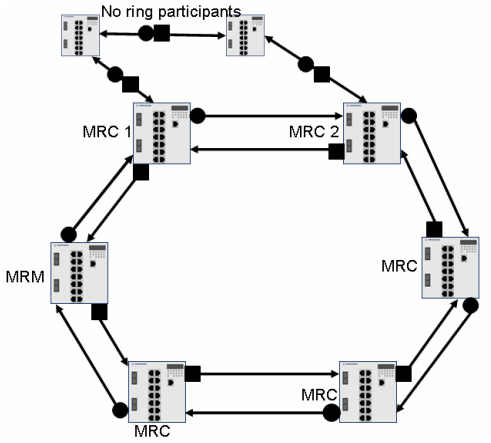

figure 4. ring with mesh

In addition to the doubly received frames on MRC 1 and MRC 2, these switches would, without any further control, forward the configuration frames to all ports they did not receive them originally. This would lead, in the long run, to a multitude of copies of configuration frames, flooding the network. So the loop detection mechanism must include means not only to detect the loops, but to remove the configuration frames themselves and prevent them from looping.

So it is necessary to save for each port of a network device the highest received sequence number and the lowest hop count for the sequence number. Per network device, a loop detection flag and a loop source identifier flag are needed. With this information in each network node, it is possible to detect loops and to detect, whether a network device is the source where a loop in the topology is originating. In figure 4, the additional mesh with the loop originates from MRC 1 and MRC 2. These two devices will be reported to the MRM as loop sources and will be identifiable by the administrator. The mechanisms how the loop detection works on each individual MRC and MRM are described in the following paragraphs.

"circle" direction			"square" direction		
port number	sequence number	hop count	port number	sequence number	hop count
1			1		
2			2		
3			3		
4			4		
...			...		

figure 6. information stored in each device

Figure 6 shows the information stored in each device in an exemplary, figurative table per port. The loop source identifier and loop detection flags are omitted in this table, they are not stored once per port but once per device. Because configuration frames travel in two directions from the two ring ports of the MRM as

described above, for the frames of each direction, one table column has to be maintained.

3.3. Configuration initialization and MRC behavior

The only device that needs to be configured by the administrator is the MRM. On this device, all relevant parameters for the ring redundancy protocol are configured. Once this is done, the automatic ring configuration is activated, and the MRM starts to send configuration frames to the ring, initiating the loop detection mechanism.

In addition to the MRM configuration, a protocol removing loops on the logical layer, like RSTP (Rapid Spanning Tree Protocol), must be activated on the devices. If the topology is a simple ring and the ring is the only loop structure present, the MRM itself immediately breaks the loop after it is being configured, but in case of additional loops besides the main ring or if the MRM is in factory default state and not blocking one ring port, a protocol like RSTP is needed to prevent loops which would overload the network. For the protocol to work properly, the configuration frames need to pass ports that are blocked by RSTP on devices that are aware to the automatic configuration protocol, similar to RSTP BPDUs (Bridge Protocol Data Units) on blocked ports of Switches that support RSTP. An MRM receiving a configuration frame will remove the configuration frame from the network and analyze the source MAC address: If the source MAC address is not its own MAC address, another MRM is present in the ring. This is a faulty configuration, because with MRP or any similar ring redundancy protocol, only one redundancy manager may be present in a ring network at any time. This fault is communicated to the administrator, who has to remove the other MRM prior to an automatic ring configuration.

An MRC, receiving a configuration frame on one of its interfaces will analyze the SDU of the frame: The sequence number and hop count are analyzed and compared to the values stored in the switch. The analysis of hop count and especially sequence number has to be done because in switching queues, frames can be reordered or if there are meshes present, multicast frames will be doubled. This could lead to possible ambiguities and misinterpretations on the devices.

The behavior of the protocol in an MRC is described as follows:

1. When a device receives a configuration frame on one port, it checks its port table and compares the sequence number of the frame received with the sequence number that is stored in the table for this port:
   a. If previously no frame with this sequence number was received on this interface and therefore the sequence number field for this port is empty or if it contains a lower value, the entry in the table is updated with the sequence number and hop count from the frame and the frame is forwarded on all ports except the port it was received at. If the entry that was created or updated was the third entry in the port table with this sequence number, the loop source identifier flag is set.
   b. If a frame with this sequence number was already previously received on this interface, the frame is dropped and the loop detection flag is set. If the hop count of the frame received is lower than the one stored, the stored value is updated with the new count.
   c. If the sequence number stored in the port table is higher than the sequence number in the received frame, the frame is dropped.
2. When the loop detection flag is set, a unicast message to the MRM is sent, reporting a network configuration which is unsuitable for automatic ring configuration. This is subsequently reported on the MRM to the administrator/operator. The MRM MAC address is known to each MRC via the source address of the configuration frame.
3. If the loop source identifier flag is set, a unicast message is sent to the MRM, indicating the device to be the source of a loop structure, which has to be removed before an automatic ring configuration can be made.

The saved information is kept for frames from both directions, there are separately saved information for the “circle” and “square” frames, as shown exemplary in figure 6.

It is possible for a loop not to be detected with this mechanism, if the frequency of configuration frames sent to the network is too high, compared to the transit time through a large network mesh. In a worst case scenario, a frame with a higher sequence number n could always arrive at a device before a duplicated frame with the sequence number e.g. n-1 or frames with the same sequence number could be received on more than two interfaces, but in a timely context that never three entries with the same sequence number could be present. This would mean that loops which introduce frame duplication would never be detected and the devices the loops originate from cannot be detected. Therefore, the sending frequency for configuration frames from the MRM must not be too high, but in a sensible range for large loops to be detected, e.g. around 20 – 30 seconds. This gives the frames ample time to be transmitted, duplicated, registered, received and removed on the individual network devices so that the port tables will be filled and the system goes into a steady state until the next configuration frame with a higher sequence number arrives. If, a new configuration frame arrives and an old frame is still circulating, the old frame will be removed when the port tables are updated with the higher sequence number, as described above.

3.4. MRM data analysis and behavior

With the data transmitted from the MRCs, the loop detection and loop source identifier information, a MRM can determine whether a consistent ring configuration is possible. The MRM will always remove any configuration frames it receives on any port. In addition, it will do the following:

1. If the MRM receives configuration frames with identical sequence numbers but different hop counts, it will detect a loop.
2. If the MRM receives a configuration frame with a port indicator on the port this frame was sent on, it will detect a loop.
3. If the MRM receives a loop detection indication frame, it will detect a loop.
4. If the MRM after three consecutive configuration frame sending operations has not received any configuration frame on its other ring port, it assumes that the ring is broken at some point and physically not closed. This error needs to be corrected before the automatic configuration can be done.
5. If the MRM has not received a loop detection indication or loop source indication frame from an MRC or has not detected a loop itself after three consecutive sent and received configuration frames, it assumes that the ring configuration can be made and it prompts the user to initiate the configuration process.

If at any point the automatic configuration fails due to a detected loop, the user will be informed to reconfigure the network. The MAC addresses from the loop source indication frames, where loops are detected, are also reported. Via this MAC address, possibly in conjunction with a network engineering tool or a network management system (NMS), an administrator can pinpoint the devices which are part of a loop structure and initiate the appropriate actions for the reconfiguration of the physical network.

3.5. Activation of the automatic ring configuration

If no additional loop is detected, the user is prompted to start the configuration process with a user command on the MRM. As soon as the user gives the command to configure the ring, the MRM sends out a configuration indication frame from both ring ports. A MRC receiving the configuration indication frame will configure the ring redundancy protocol for the previously received parameters and after the configuration is done and the device is ready to participate in the ring, the frame is forwarded on the other ring port.

As soon as the MRM receives both configuration indication frames on both its ring ports, it assumes that the ring is configured and ready for normal operation. It will then assume normal ring operation according to the ring redundancy protocol configured.

3.6. Devices which do not support the protocol

Devices which do not support the protocol may be present either in trees or meshes outside the desired ring or may be ring devices.

In the case the devices are present in trees connected to protocol sensitive devices that are part of a future ring, the loop detection mechanism on the corresponding ring device will be unaffected. In case a whole tree consists of devices unaware to the protocol, potential loops in the tree substructure will be administrated via RSTP or a similar protocol, while the devices not aware to the configuration protocol will treat the configuration frames like standard MAC multicast frames.

In the case that they are ring devices, this is a critical installation fault that cannot be detected via the configuration protocols detection mechanisms alone. In this case, the automatic configuration cannot be realized. A detection mechanism to identify protocol unaware devices on the ring via the protocol alone is not possible, as these devices are completely transparent to the protocol and therefore to any detection mechanism. Such a faulty configuration can be detected, if a NMS is used to monitor the network devices and to map a network topology.

With Hirschmann devices, neighbor device detection is implemented using the industrial standard protocol LLDP [12]. LLDP is also implemented in Profinet devices compliant to conformance class B or higher. If there is no NMS in use to support the detection of network devices not supporting the protocol, LLDP can be used for device and capability detection [4]. But generally, a setup with a protocol unaware device shall be prevented from the start with a correct physical device setup.

3.7. Devices with limited protocol support

In case a device has just exactly two distinguished ports, it can implement the protocol with just the ability to extract protocol configuration parameters from the configuration frames and to forward the configuration indication frame. This can be implemented e.g. on common field level Profinet I/O devices with two ports, offering MRP MRC support. This enables a slim protocol implementation on I/O devices with very low resource consumption.

4. Security: Protection against misuse

While configuration protocols often provide quick and comfortable ways to configure network devices with little effort, there is always the possibility of misuse and sabotage.

In order to sabotage a network already in operation, a denial of service attack with a very high number of configuration frames sent to the network could be done to overload the devices. This is prevented with a

mechanism to limit the number of actually received and processed configuration frames to a defined low number.

Additionally, as a first step to secure a configured and running installation against protocol frames inserted by an attacker with malicious intend to reconfigure the ring devices and to interrupt normal ring operation, the automatic ring configuration will be locked on all MRCs once the ring configuration is done. This lock can be released by connecting to each MRC individually and authenticate via command line, web interface login or via SNMPv3 (Simple Network Management Protocol Version 3). This assures that only service personnel with correct login credentials can manipulate the switch configuration. There is a distinct disadvantage to this: To reconfigure a network or to initiate a new automatic ring configuration cycle once the network is in operation, a manual operation on each ring device is necessary.

To circumvent this, in future versions of this protocol, an authentication mechanism is planned between an MRM and the individual MRCs, reducing the actions needed to initiate another configuration cycle to the user authentication on the MRM.

5. Application to a use case

Figure 7 shows a fictional network to which the automatic ring configuration will be applied. The MRM is marked with "MRM" and all MRCs are given characters for identification. The first step of the automatic configuration is that the administrator configures the MRM with all necessary ring protocol parameters and initiates the automatic configuration process by starting the ring check. The MRM will then send out configuration frames from both its ring ports, in order to deliver the parameters of the protocol to the MRCs and to check if the topology is, with exception of the ring to be configured, loop free.

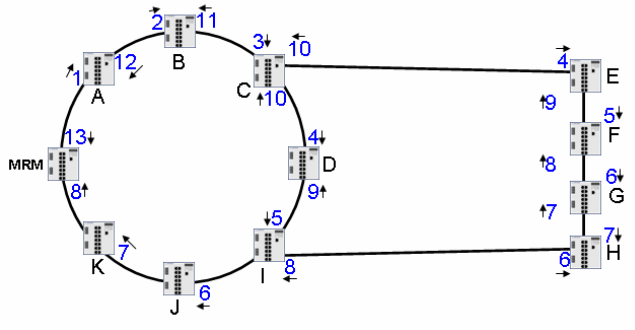

figure 7. ring structure with mesh

In figure 7, only the paths a configuration frame sent from ring port 1 of the MRM, in this case on the network connection going upward towards MRC "A", are displayed. The paths a configuration frame takes from MRM ring port 2 are not displayed so it is possible to keep track of the frame from port 1 and subsequently the frames that are additionally. The mechanism works the same way for the frame from MRM ring port 2, just the other way around.

Figure 8 shows the path of the frame(s) in a tree-like structure, where a branch in the tree indicates a frame multiplication. The frame travels on a step-by-step basis, the switching times and line delays in the network are assumed to be virtually identical between all devices and links. In a real world network, this will not be the case and the "tree" in figure 8 might look different. A step in figure 8 can also be interpreted as the hop count after ingress and increment in the respective device. The steps and ingress directions are displayed in numbers and with small arrows in figure 7.

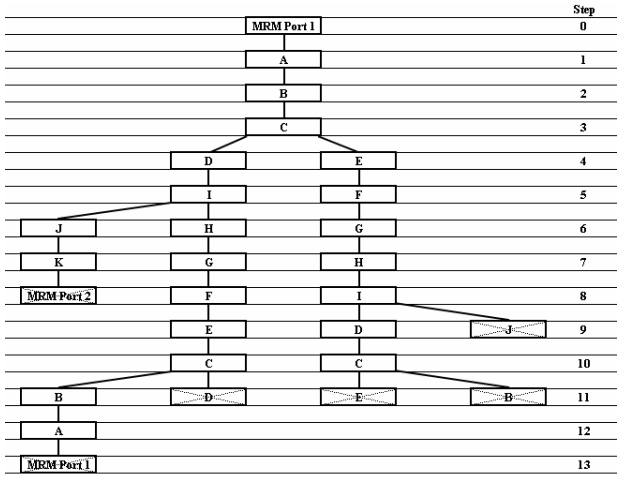

figure 8. travel paths of configuration frames

The frame starts off from MRM Port 1. In MRC "C", it is multiplied for the first time, traveling to "D" and "E". As described in 3.3, on each ingress of a frame, its sequence number is recorded for this port. The frame traveling from "C" is again multiplied in "I", and also travels towards the MRM Port 2, where it is removed from the network, indicated by a crossed-out box in figure 8. It also marks all ingress ports on this network path with its sequence number, and in the future, no other frame with the same sequence number can travel this network path, but will be removed. The frame multiplications can be observed when following the paths of the frames in figure 7 and figure 8. A special case comes up in step 10, where frames from "E" and "D" arrive at identical step count on different ports. It is non-deterministic, which frame will arrive first and will be processed first. In this example, it is assumed that the frame from "E" did arrive first and travels all the way back to MRM Port 1. The second frame will be received and transmitted, but will be removed on the following devices. MRC "C" can therefore, by the ingress of one frame with an identical sequence number on 3 or more ports, be identified as the source of a loop and will send the loop source indication to the MRM. MRC "I" cannot be detected as a loop source in this direction, but will be

identified by the frame traveling from MRC port 2 in the opposite direction. With many devices sending the loop detection indication and loop source indication, the administrator will not be able to continue with the automatic ring configuration. He or she has to remove one physical loop, e.g. by administratively (temporarily) blocking a port on MRC "C" or by removing physical connections if they were not intended in the original network design. The additional use of a NMS that can graphically map a network topology or a Profinet engineering tool can be of great use here. After the loop is removed, the configuration can be started again. If no loop was detected on the MRM after three consecutive configuration frames sent and received, the administrator can activate the ring configuration.

6. Implementation in Ethernet Switch Software

The automatic ring configuration is intended to be part of the next major release of Hirschmann Ethernet Switch Software. In the software itself, the functionality will be called "ARC", short for "Automatic Ring Configuration". Like with most switch functionality in Hirschmann devices, the protocols configuration and saved parameters are accessible via SNMP through a dedicated MIB (Management Information Base). A new MIB for the ARC has been written, containing all protocol parameters and a list item for MAC addresses that have been identified as sources of a loop via the loop detection flag described earlier. This information can then be accessed via SNMP to be used in a NMS. The information is also used by the web user interface of the devices. If a device fulfills the MRM role, the ARC can be initiated in the same dialogue where the ring redundancy is being configured.

7. Summary

The automatic ring configuration offers a quick and easy way to configure many ring devices at once with only a few configuration steps necessary. This aids administrators by saving time in configuration processes and enables the possibility of ring redundancy configuration for application specialists who want to use redundant Ethernet network structures, but don't want to be burdened with an elaborate configuration process.

The automatic ring configuration has the ability to detect whether it will work in a certain network layout, but, like with a manually configured network, precautions in the deployment of actual physical network devices have to be made in order not to mix devices not supporting network protocols with devices supporting it.

The automatic ring configuration is especially useful in application scenarios where the installation follows the network structure which is intended with ring redundancy protocols: one ring with simple leaf links or connected trees. In these network structures, the protocol immediately detects and configures network devices that are part of the desired redundant ring structure.

References

[1] Prytz, G.; "Redundancy in Industrial Ethernet Networks", *Factory Communication Systems, 2006 IEEE International Workshop* on June 27, 2006 Page(s):380 - 385

[2] Kirrmann, H.; Dzung, D.; "Selecting a Standard Redundancy Method for Highly Available Industrial Networks", *2006 IEEE International Workshop on Factory Communication Systems*, June 27, 2006 Page(s):386 – 390

[3] IEC 62439: "Industrial communication networks: high availability automation networks", CDV distributed on 2008-11-21 available at www.iec.ch

[4] Schafer I., Felser M.: "Topology Discovery in PROFINET", *12th IEEE Conference on Emerging Technologies and Factory Automation*, 2007. ETFA 2007, September 25-28, Patras, Greece

[5] Kleineberg O., Felser M.: Network Diagnostics for Industrial Ethernet, 13th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2008); September 15-18, 2008, Hamburg, Germany, Work in Progress

[6] Rentschler, M.; Maisch, W. - Patent Nr. US020080250124A1 - [EN] Redundancy-protocol configuration in a ring network

[7] IEC 61158-6-10: "Industrial communication networks – Fieldbus specifications – Part 6–10: Application layer protocol specification – Type 10 elements", available at www.iec.ch

[8] IEC 61158-5-10: "Industrial communication networks – Fieldbus specifications – Part 5–10: Application layer service specification – Type 10 elements", available at www.iec.ch

[9] IEC 61784-2: "Industrial communication networks – Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3", available at www.iec.ch

[10] PROFIBUS International: "PROFINET: Technology and Application, System Description", Document number: 4.132, Issue April 2006, available at http://www.profibus.com

[11] Felser M.: Media Redundancy for PROFINET IO, IEEE Workshop of Factory Communication Systems 2008, Dresden, 20 to 23rd May 2008, Pages 325 to 330

[12] IEEE: IEEE 802.1AB-2005 - IEEE Standard for Local and metropolitan area networks Station and Media Access Control Connectivity Discovery; available at www.ieee.org