Smart Grid and Renewable Energy, 2016, 7, 147-153
Published Online April 2016 in SciRes. http://www.scirp.org/journal/sgre
http://dx.doi.org/10.4236/sgre.2016.74011

The Parallel Redundancy Protocol over Wide Area Networks

Martin Stefanka

ABB Inc., Lake Mary, USA
Email: martin.steafanka@us.abb.com

Received 22 February 2016; accepted 22 April 2016; published 25 April 2016

Abstract

To accomplish the safety-critical mission of transmission and distribution automation, high availability and stability are always required in the industrial communication networks. The IEC 62439 Standard (Industrial communication networks-High availability automation networks) Part 3 defines the Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) protocols. Both redundancy protocols target the process bus described in IEC61850 9-2 [1] and support only Local Area Networks (LANs). It has become an active research area to extend the redundancy protocols to the Wide Area Network (WAN) communication with existing network infrastructure. This paper offers a novel solution, namely the parallel redundancy protocol over the wide area networks (PRPW), to enable PRP over WANs with no added overheads to the data frame, while retaining full compatibility. Moreover, PRPW also strengthens the cyber security against spoofing attacks by maintaining a comprehensive list of remote communication units.

Keywords

PRP, WAN, LAN, IEC 61850, Industrial Ethernet

1. Introduction

The modern transmission and distribution automation system relies on various types of communication, e.g., control data exchanged between the substation and the remote control center, protection data shared within the bay level, sample data sent from measuring devices to the intelligent electronic devices (IEDs), control command sent from IED to the switch gear, etc. Among those, some local communication, e.g., sensors reporting the sample values of voltage and current to an IED/IEDs in the same substation, goose messages exchanged between IEDs, are limited within the LANs; whereas other communication, e.g., the control and protection data exchanges between the IEDs and the supervisory control and data acquisition (SCADA) system or next generation centralized protection and control (CPC) units, may need to travel through WANs.

How to cite this paper: Stefanka, M. (2016) The Parallel Redundancy Protocol over Wide Area Networks. *Smart Grid and Renewable Energy*, **7**, 147-153. http://dx.doi.org/10.4236/sgre.2016.74011

To fulfill the stringent reliability requirements of communication while maintaining the interoperability of IEDs in Substation Automation Systems (SAS), IEC 62439-3 [2] defines two redundancy protocols, Parallel Redundancy Protocol (PRP) (IEC 62439-3 Clause 4) and High-availability Seamless Redundancy (HSR) (IEC 62439-3 Clause 5). Both of the two redundancy protocols are capable of overcoming the failure of a link or a switch in a network with zero switchover time, while enabling clock synchronization according to IEEE 1588 (v2) [3].

The two protocols employ different approaches and infrastructures. The PRP protocol duplicates the data frames to be transmitted, patches a redundancy control trailer (RCT) with a unique sequence number to the end each of the frames, and sends them through two independent similar-topology LANs (IST-LANs). The receiver identifies the frames by the RCT and the source MAC address, accepts and processes the first arrival data frame, and then discards the second if it ever comes.

Since the RCT is patched at the end of the content of a data frame, it can be ignored by the PRP non-compatible equipment. This approach ensures that the PRP protocol works with both PRP compatible and non-compatible equipment as long as the transmitter and receiver ends are PRP compatible.

Similarly the HSR protocol duplicates a data frame and sends both data frames through both directions to a ring-topology local area network (RT-LAN). On the ring, each device incorporates a switch element that decides to either forward or discard the frames from one port to the other. However instead of patching at the tail, HSR protocol inserts a header between the MAC header and the payload of the data frame. Consequently, the HSR tagged data frames will be processed only by the HSR compatible network equipment, and dropped as bad frames by HSR non-compatible equipment.

The HSR/PRP protocols are designed for and will only benefit the communication within the LANs for the fact that the source MAC address of the data frame, used with a sequence number (assigned by HSR/PRP) as a unique doublet to make forward/discard decisions, will be alerted and lose its uniqueness when transferred from the LANs to the WANs. Consequently, even redundancy protocols are enabled within the LANs at both ends; the communication through the WANs could experience a long recovery time if the LANs are connected to the WANs with redundant routers, or even suffer single point failure if each LAN is connected to the WANs with a single router.

Therefore, it has become a new research focus on how to adapt the state of art LAN redundancy protocols, especially the PRP, to support WAN communication with existing network structure. The PRP gains its popularity in the WAN adaptation for two reasons. First, PRP offers better compatibility and interoperability with non-redundancy equipment in the existing WANs. Second, with a quad box, the data frames from HSR LANs can be converted to PRP data frames as described in the IEC 62439-3 standard.

One approach is presented by M. Rentschler and H. Heine by modifying the RCT to extend the PRP to the WAN [4]. But their solution is not fully compatible with current PRP protocol and also increases the overhead by patching more bytes.

In this article, a solution to adapt the PRP to WAN communication is proposed, namely the PRP over WAN (PRPW). The PRPW embeds the originator's MAC information in the RCT to keep its integrity during the WAN transmission, and recovers it at the receiver end. The PRPW maintains fully compatibility with PRP while enhancing the system's cyber security by monitoring, logging and reporting the spoof attack.

In the rest of the paper, PRP and its RCT will be introduced in Section 2. The WAN routing and its impact to PRP will be elaborated in Section 3. In Section 4, the PRPW algorithm and flow chart will be discussed. The last but not least, conclusion will be presented in Section 5.

2. Parallel Redundancy Protocol and Redundancy Control Trailer

As described in the IEC 62439-3 [2], to achieve the redundancy, the PRP nodes are connected to two independent similar-topology Local Area Networks (IST-LANs), *i.e.* L_A and L_B, through two independent physical ports as doubly attached node obeying to PRP (DANP). Those two ports share the same MAC address but operate in parallel and are attached to the same upper layers of the communication stack through the link redundancy entity (LRE) embedded in the Data Link Layer, as shown in **Figure 1**. The LRE ensures that the upper layers are unaware of and unaffected by the redundancy.

The LRE performs two key tasks, *i.e.*, handling of duplicates and managing the redundancy. After receiving an IP datagram from the upper layer, the Data Link Layer interface attaches a MAC header to the datagram and converts it to a Data Link Layer data frame, as in non-redundant networks.

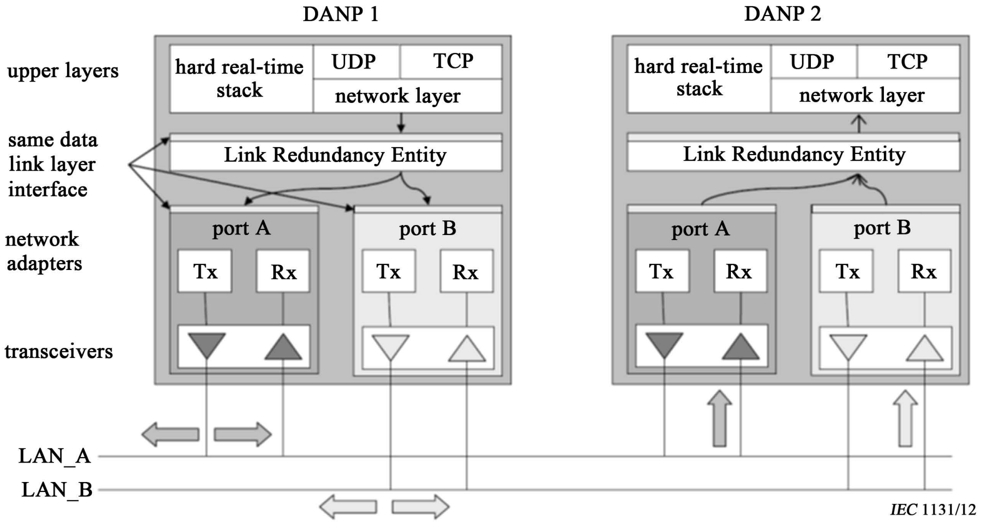

Figure 1. PRP with two DANPs communicating.

Next, the LRE duplicates the data frame, appends a redundancy check trailer (RCT) to each of the frames, which contains the PRP specific information, including a sequence number, LanID, frame size, and PRP suffix (as shown in **Figure 2**). The two RCTs are identical except for the LanIDs, *i.e.*, “1010” for L_A and “1011” for L_B. Then the two frames are sent through two physical ports to L_A and L_B separately.

The two frames travel through L_A and L_B with different delays and, ideally, both will reach the destination. The receiver DANP consumes the first frame and discards the second one (if it arrives). During the handling of duplicated frames, the sequence number in the RCT combined with the source MAC address are used as the identifying doublet of the data frame. Since the trailer will be ignored by the PRP non-compatible equipment, a standard Ethernet unit is fully functional in the PRP network as a singly attached node (SAN).

HSR has a similar mechanism of providing redundancy. However, different from PRP, HSR inserts a header to the MAC frame. This header will neither be understood nor ignored by the HSR non-compatible node, and cause the data frame to be discarded.

Nevertheless, both of the two protocols are designed for the LAN and need the source MAC address to identify the received frames. Neither of the two redundancy protocols supports WAN. Because when data frames are transmitted to the WANs, the gateways, usually Layer 3 routers, will replace the original source MAC address with their own MAC addresses during the process of routing and forwarding the data frames. This process will be elaborated in the following section.

3. Consequence of WAN Routing to Parallel Redundancy

As a LAN protocol, PRP utilizes MAC address, commonly employed by Layer 2 protocols, e.g. Rapid Spanning Tree Protocol (RSTP) [5], to identify the source and destination of the data frames. However, when a data frame leaves its original LAN through a router, the source MAC address will be replaced with the router’s MAC address, therefore lose its “identification role”. The IP address in the Layer 3 header, rather than the MAC address, will take the role of “identification address” and decide the routing hop-by-hop when the data frame reaches WAN with Layer 3 routing protocols, e.g., Address Resolution Protocol (ARP) [6]. The MAC address will regain its power when the data frame reaches its destination LAN. However, at this moment, the source MAC address of the data frame will be the MAC address of the router connecting the destination LAN to the WAN; and the originator’s MAC address of the data frame is already lost in the transmission.

For a network shown in **Figure 3**, two IEDs IED_A and IED_B are connected to the WAN through two routers and two paths of wired and wireless WANs. The wired path includes a switch and a router R_A, while the wireless path only includes a wireless router WR_A. The SCADA system also is connected by a wired path, *i.e.*, router R_B and a Layer 2 switch, and a wireless path through the wireless router SR_B. (In case of single router connection, the process is similar. However, it will cause single point failure problem, therefore is not preferred and not elaborated.)

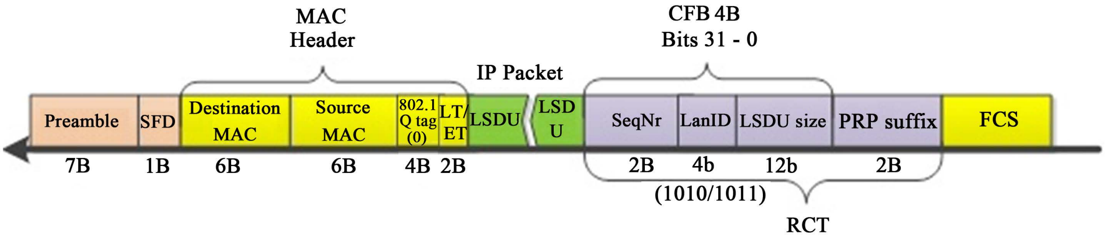

Figure 2. PRP frame extended by an RCT.

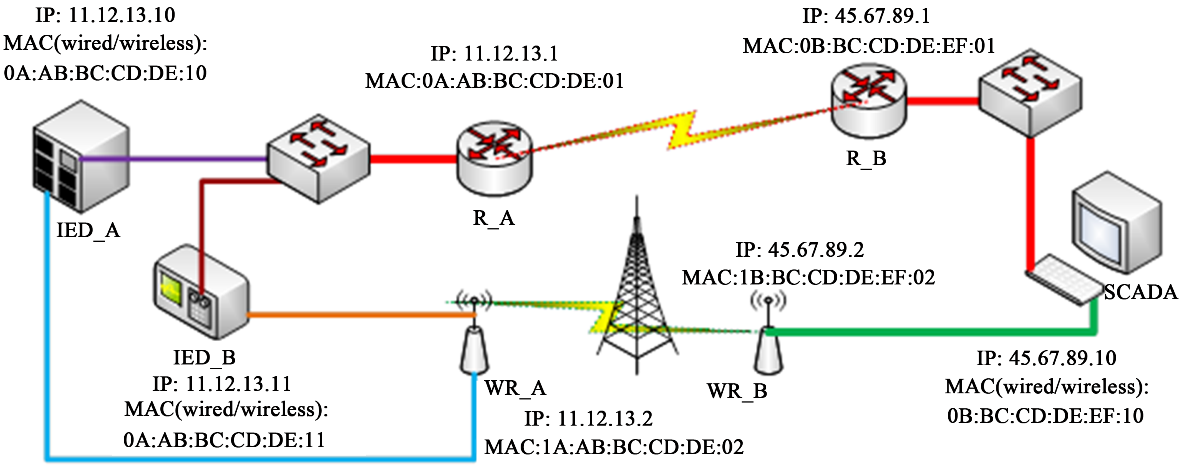

Figure 3. PRP through WAN structure.

3.1. Scenario 1

IED_A's IP address and MAC address for both ports is identical, *i.e.*, IP address 11.12.13.10 and MAC address 0A:AB:BC:CD:DE:10. The IED_A tries to the SCADA a pair of duplicated PRP data frames with the sequence number n. It will be processed as following steps:

1) From its own IP address (11.12.13.10) and the subnet mask (255.255.255.0), IED_A realizes the SCADA is on a different LAN (45.67.89.10).
2) For the wired path, IED_A sends an ARP request to find out the MAC address of its default gate way, *i.e.*, the router R_A.
3) IED_A sends one of the duplicate data frames to R_A with its own wired MAC address (0A:AB:BC:CD:DE:10) as the source MAC address and the R_A's MAC address (0A:AB:BC:CD:DE:01) as the destination MAC address. The switches pass the frame without modifying the MAC addresses.
4) The data frame is routed from R_A to R_B hop by hop. Until R_B receives the data frame, it sends the data frame to the SCADA with the R_B's MAC address (0B:BC:CD:DE:EF:01) as source MAC address and the SCADA's MAC address (0B:BC:CD:DE:EF:10) as the destination MAC address. The SCADA will receive the data frame with the identifying PRP doublet, MAC address 0B:BC:CD:DE:EF:01 and sequence number n, and LanID 1010.
5) Similar process happens to the wireless path, WR_B's MAC addresses is used instead. The SCADA will receive the data frame with PRP doublet, MAC address 1B:BC:CD:DE:EF:02, sequence number n, and LanID 1011.
6) Since the two data frames have different PRP doublets, both data frames will be forwarded to the up layers, where the TCP layer has to discard the one arriving later. This compromised the data frame discarding policy of PRP protocol and increases the overhead of processing the data frames in the upper layers.

3.2. Scenario 2

Consider both IED_A and IED_B send data frames to the SCADA.

1) At a moment, IED_A sends two PRP frames to the SCADA with a sequence number m, the data frames will be denoted as DF_A_LA (data frame from IED_A through path L_A) and DF_A_LB.
2) After a very short period (short than twrap Min, the minimum possible time between two repetitions of the same sequence number by legitimate frames after 65536 increments, about 400ms in a 100Mbit/s network), IED_B sends two PRP frames with the same sequence number m, denoted as DF_B_LA and DF_B_LB.
3) The SCADA will receive DF_A_LA and DF_B_LA with the same doublet, the MAC address 0B:BC:CD:DE:EF:01 and sequence number m. Since DF_A_LA comes first, according to the PRP discarding policy, the DF_A_LA will be forwarded to the up layer and DF_B_LA will be discarded. Similarly, DF_A_LB will be forwarded and DF_B_LB discarded.
4) As describe above, both data frames from IED_A will be forwarded, whereas both data frames from IED_B will be discarded.

Above two scenarios demonstrate the consequences of employing PRP over WAN. The acceptance of duplicate frames and rejection of legitimate frames are caused by the alerted source MAC address during the WAN transmission.

4. Parallel Redundancy Protocol over WAN (PRPW)

When extending the PRP to WAN, retaining the original sender's MAC address is the key issue. The PRPW offers such a solution with full compatibility with current PRP protocol, as shown in **Figure 4**.

The PRPW solution is elaborated as follows:

1) A MAC address list of remote DAN, where remote is defined as outside the current LAN. The MAC address list is created by the engineer during the initialization process and updated when necessary, e.g., when new remote DANs need to be connected or existing DANs need to be replaced.
2) The MAC address will be calculated with a hash function, which translates the 6-byte MAC address to a 4-byte Hashed-MAC address (HMA).
3) Before an IED sends the data frames, it checks whether the destination MAC belongs its local router (The router's MAC address can be obtained and updated with ARP protocol). If not, the receiver is within its current LAN, and the sender will send the two PRP data frames directly. Otherwise, the sender will modify the first 4 bytes of the RCT (SeqNr + LanId + LSDUsize), noted as the Characteristic Four Bytes (CFB) in the rest of the paper, by XORing the CFB with the sender's own HMA, and then send the modified data frames through the two physical ports.
4) For each received data frame, the receiver will check whether the RCT contains a valid LanID, which should be either 1010 or 1011. If a valid LanID is found, it is a local PRP data frame and will be treated with standard PRP process. Otherwise, it is a PRPW frame.*
5) For a PRPW frame, the receiver will XOR the CFB with each MAC address in the MAC address list of remote units, until a valid LanID is generated or to the end of the list.
6) If a valid LanID is generated in the previous step, the RCT of the received data frame should be replaced with the result of XOR operation, and the source MAC address should also be replaced with the corresponding MAC address in the remote units list. The modified frame will be processed, *i.e.*, forwarded to the upper layer or discarded, as a standard PRP frame. (In this step, instead of replacing the router's MAC address with the originator's MAC address, the PRPW protocol can use the originator's MAC address to make its own decision of forwarding or discarding, and retains the router's MAC address for other protocols.)
7) If none of the HMA in the remote units list can generate a valid LanID in step 5, the data frame should be forwarded to the upper layer with an increment in the error counter.**

*For the sender, to avoid accidentally generating a valid local LanID for remote receivers, the hash function should not generate a HMA with the corresponding bits to the LanID (bits 15 - 12) as "0000" or "0001" (as shown **Table 1**). If the hash function does not limit its output, the receiver should check if the source MAC address of the received data frame is one of its local routers' to decide whether the data frame is from LAN or WAN.

**Since it could be a configuration error either on the sender's side or on receiver's to cause the invalid LanID in step 7, e.g., a missing MAC address in the remote unit list, the payload of the data frame can still be valid. Therefore, the data frame with invalid LanID will be forwarded to the upper layer for future decision. Because this type of configuration errors is permanent, they can be detected rapidly by monitoring the error counter.

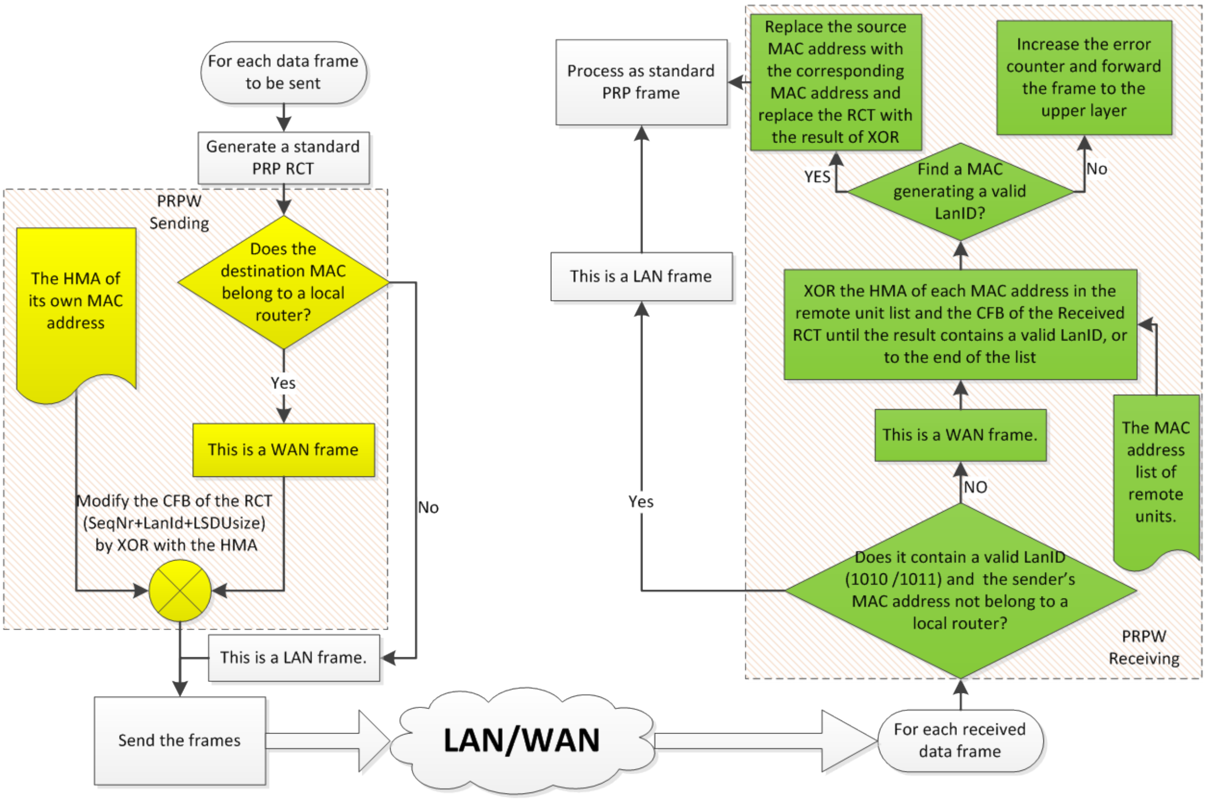
For each data frame to be sent
Generate a standard PRP RCT
PRPW Sending
The HMA of its own MAC address
Does the destination MAC belong to a local router?
Yes
This is a WAN frame
Modify the CFB of the RCT (SeqNr+LanId+LSDUsize) by XOR with the HMA
No
This is a LAN frame.
Send the frames
LAN/WAN
For each received data frame
Process as standard PRP frame
This is a LAN frame
Yes
Replace the source MAC address with the corresponding MAC address and replace the RCT with the result of XOR
Increase the error counter and forward the frame to the upper layer
YES
Find a MAC generating a valid LanID?
No
XOR the HMA of each MAC address in the remote unit list and the CFB of the Received RCT until the result contains a valid LanID, or to the end of the list
This is a WAN frame.
The MAC address list of remote units.
NO
Does it contain a valid LanID (1010 /1011) and the sender's MAC address not belong to a local router?
PRPW Receiving

Figure 4. PRPW Solution flow chart.

Table 1. Combinations of HMA bits 15 - 12 that retain valid LanID with XOR operation.

Hashed MAC Address (HMA)	LanID	HMA XOR LanID
0000	1010	1010
0001		1011
0001	1011	1010
000		1011

Moreover, since the spoof attacker may not have the MAC address list of the remote units, the spoof attack could also be detected efficiently with the same manner.

5. Conclusion

This paper presented a PRP over WAN solution, namely PRPW, to extend the PRP protocol to the WAN without increasing the overhead of the data frames. The PRPW protocol maintains a complete compatibility with current PRP protocol and can fully utilize the existing network, LANs and WANs. It can also be utilized to extend HSR networks over the WAN with quad boxes. The employing of MAC address list of remote nodes enhances the system's cyber security by monitoring, logging, and reporting spoof attacks.

Acknowledgements

I wish to acknowledge the excellent support I received from Dr. Xiaoguang Ma for his great work on all testing experiments what comes to PRP over WAN.

References

[1] IEC 61850-9-2 (Edition 2.0 2011-09) Communication Networks and Systems for Power Utility Automation—Part 9-2: Specific Communication Service Mapping (SCSM)—Sampled Values over ISO/IEC 8802-3.

[2] IEC 62439-3 (2012) Industrial Communication Networks—High Availability Automation Networks. Part 3: Parallel Redundancy Protocol (PRP) and High Availability Seamless Redundancy (HSR).

[3] Kirrman, H. (2010) Special Report IEC 61850-ABB, Seamless Redundancy Bumpless Ethernet Redundancy for Substations with IEC 61850.

[4] Rentschler, M. and Heine, H. (2013) The Parallel Redundancy Protocol for Industrial IP Networks. 2013 *IEEE International Conference on Industrial Technology* (*ICIT*), Cape Town, 25-28 February 2013, 1404-1409. http://dx.doi.org/10.1109/ICIT.2013.6505877

[5] 802.1w—Rapid Reconfiguration of Spanning Tree. http://www.ieee802.org/1/pages/802.1w.html

[6] Plummer, C. (1982) An Ethernet Address Resolution Protocol. RFC 826. http://tools.ietf.org/pdf/rfc826.pdf