Station Reconfiguration on FDDI Trunk Rings

William S. Hiles and David T. Marlow
Engineering and Technology Division
Combat Systems Department
Naval Surface Warfare Center
Dahlgren, Virginia 22448-5000

Abstract

The U.S. Navy is selecting a set of Local Area Networking standards, under the name SAFENET, for use on tactical platforms. The set of standards incorporate the FDDI Local Area Network (LAN) at the Physical and Data Link layers. The SAFENET group has taken an FDDI feature (the Hold Policy option) initially developed to support transferring data on FDDI's dual counter-rotating trunk rings simultaneously and has used it as the basis of a data path hop (or switch) capability. This paper provides a discussion of FDDI trunk ring reconfiguration both in a normal mode of operation (i.e., the Hold Policy not in effect) and when the Hold Policy is in effect. Operational issues of concern to tactical network survivability are discussed. A discussion of the issues that result from the use of optical switches, the use of the Hold Policy, the use of dual Media Access Controllers, the resolution of addresses and the association of one data path to one of two Media Access Controllers is provided.

1 Introduction

The U.S. Navy is in the process of selecting a standard profile of protocol standards for the use of Local Area Networks in tactical systems. The Survivable Adaptable Fiber Optic Embedded Network (SAFENET) profile specifies the Fiber Distributed Data Interface (FDDI) standards for the physical [1,2] and data link layers [3] of the OSI model. A major concern for this profile of standards is to ensure high availability and in particular survivability of the data path after a tactical platform has sustained battle damage [4].

While the FDDI topology is a “ring of trees” as shown in Figure 1, the current SAFENET MIL Handbook [5] calls out a topology of directly connecting all user nodes (i.e., stations) via dual counter-rotating FDDI trunk rings with the Hold Policy option of FDDI active. Typically an FDDI network which contains dual rings passes user data on only one ring at a time, utilizing the other ring in the case of failure for wrapping around inoperable stations or cables. The Hold Policy option was developed to utilize the dual rings simultaneously in which case it is desirable to prevent the wrapping operation if at all possible. The SAFENET MIL Handbook draft specifies that only one of the rings at a time will transfer user data but utilizes the Hold Policy as a means of enabling additional reconfiguration capabilities. The SAFENET MIL Handbook draft provides additional specifications, on top of the protocols provided within the FDDI Station Management standard [6], to implement a means of either holding on a surviving ring or hopping (or switching) to the alternate ring as the first line of action upon an interconnection fault. The wrapping of the two rings is performed as the last resort.

Concerns over the actual capabilities of the SAFENET reconfiguration specifications has lead to a study effort which is presently on-going within the SAFENET Working Group where alternative or additional reconfiguration methods may result. During this study effort a report was written [7] which covered the details of the present SAFENET reconfiguration method. The focus of the report and this paper is to describe the capabilities of reconfiguration on FDDI trunk rings supporting one active data path and using the standard FDDI features. Issues identified through the SAFENET study will be addressed in generalized terms. Issues unique to the use of FDDI concentrator based reconfiguration schemes are not covered.

2 FDDI Trunk Ring Operation

FDDI is a token passing LAN which specifies a “ring of trees” topology where user systems can be connected ei-
ther directly to the dual counter-rotating trunk ring or through concentrators. Interconnecting directly to the trunk rings provides additional reliability since the second ring can be used in reconfiguration operations. The two rings may or may not transfer data simultaneously depending on the types of stations attached to the network. The FDDI standard does not preclude using the dual rings for transferring data simultaneously but a networking profile such as the Navy’s SAFENET MIL Handbook may preclude this (and does). For the case of using one data path at a time on the trunk ring, data is passed from station to station in a circular fashion using the token passing arbitration scheme for access to the network. In the event that a cable is broken or disconnected, the two rings are wrapped (i.e. joined) to form one larger, but continuous ring. Figure 2 shows a simple three station ring before and after a fault on the network.

![Figure 2a: Normal operational FDDI ring](image)

![Figure 2b: Ring state after reconfiguration due to segment fault](image)

Figure 2 illustrates a number of points for this type of FDDI network. Given that data is transferred across one path at a time a dotted line is shown for the paths not used in the active data path. Also, the figure shows that the FDDI topology utilizes counter-rotating rings. The data on the outside ring flows in a clockwise fashion and the data on the inner ring flows counter-clockwise. This is required for the reconfiguration scheme to work effectively. After the fault on one of the links, the stations around the fault perform what is called a WRAP. Basically, the data is internally wrapped back to the second ring. This allows the network to continue to operate even with a single fault. Once the fault is corrected, the network will reconfigure itself automatically using protocols defined in the FDDI SMT standard.

Although the ability to recover from a single fault is the primary benefit from this type of counter-rotating ring topology, a serious problem does exist. If two faults occur on the network, stations may be isolated and independent rings may form. This problem of segmentation is illustrated in Figure 3.

![Figure 3a: Examples of a segmented ring due to two breaks on the primary](image)

![Figure 3b: Examples of a segmented ring due to a break on both rings](image)

The problem of isolation is serious for many applications including tactical systems. When an event occurs which involves battle damage, platform-wide problems may result in forcing a single FDDI ring to end up as a group of isolated rings. Many of the problems may be short-lived in the case of transients of less than a second and power-outages that might last minutes. When a network is segmented, the isolated stations form a fully operational ring and cannot access stations on other rings. As long as the fault does not separate communicating systems, the isolated groups may be able to carry out their functions adequately. However, isolation of communicating systems can result in system failure.

### 3 Use of Optical Bypasses

If all stations in a FDDI ring are not powered up, the trunk ring will be wrapped and perhaps segmented depending on the locations of the stations which are up. A station which is powered down breaks the ring because light does not propagate through the station. To solve this problem, networks can be built with optical bypasses for station connections which can physically remove the sta-
tion from the optical paths of the rings. When a station is powered down and no power is provided to the bypass, it will automatically be placed in the "bypass" state. Optical signals are then passed around the station and thus other stations are permitted to come up in a normal ring. The key point is that the optical bypass is a passive device which does not require power to accomplish the bypass state.

Optical bypasses also present problems for networks. A major problem is the signal loss at the bypass. Typically, each bypass and its associated connectors will present a loss of 2 to 3 dB in the optical path. The FDDI specification for maximum allowable attenuation between any two stations is 11 dB. Obviously if a ring has 10 stations and only two are powered up, the optical bypasses will induce too much loss for the ring to operate forcing it to wrap. At least every third station must be powered up and inserted in order for the ring to operate normally. The benefits of using optical bypasses must be considered on a case by case basis. The SAFENET MIL Handbook specifies that all stations on the trunk ring must be connected through optical bypasses which are closed (i.e. the station bypassed) when no power is applied to the bypass and has specified a larger power budget to allow more stations to be powered down before causing a WRAP condition.

The optical bypasses available today are susceptible to damage after a high impact shock. Militarized bypasses are being developed; however, these still experience transient effects where the LAN is disrupted temporarily. In addition, if a station is experiencing problems which cause the bypass to oscillate (alternating between the through and bypassed states), the FDDI network will reconfigure with every bypass transition. This particular problem is disruptive to the network since data does not flow on the ring during reconfiguration and if the period of oscillation is rapid, the ring may never become operational.

Optical bypasses add additional cabling to a network which creates additional requirements for cable routing and maintenance. The bypass requires additional fiber optic connections as well as electrical cabling to control the switching mechanism. The additional fiber optic cable is either spliced or uses connectors that contribute to the signal attenuation. This extra cabling must be considered in the overall plan of the network and the locations of the optical bypasses must be considered to ensure that the bypasses do not become likely points of failure for the network. In applying this technology to specific designs, it has been found that certain rooms or compartments have required many LAN interconnections. One solution is to incorporate a number of bypasses within a single enclosure and provide one bypass for the entire enclosure. Signal amplification can be added internally as long as the signal is regenerated using electronics which provide error correction and checking. This approach can aid in providing a practical solution for the signal loss problem; however, in this case, the solution is not totally a passive system.

4 Use of the Hold Policy

The current SAFENET MIL Handbook draft specifies the use of the Hold Policy within the FDDI SMT specification for all SAFENET networks in an attempt to increase the survivability of the network. The Hold Policy within the FDDI standard is optional and was developed for high-end commercial applications to allow for transfer of data on both rings at the same time. No commercial products have emerged or have been announced which incorporate the use of both rings for data transfer at the same time. The use of the Hold Policy requires that the stations implement a dual-MAC architecture for all stations. The addition of the hardware for a second MAC and the necessary glue logic and software may greatly increase the cost of network nodes. It is important to understand the operational benefits.

Essentially, the Hold Policy disables the reconfiguration capability of the FDDI ring until faults occur on both rings. The actual mechanism for doing this is very simple but does cause other problems. The normal cables used for FDDI have the two fibers for the rings housed in one cable. With this configuration, an event which breaks the path of one ring usually means a fault on both rings. The Hold Policy increases the survivability of the network provided that the primary and secondary rings are routed separately as specified in the current SAFENET MIL Handbook draft.

When a single data path is used and the network experiences a break on the active ring, the Hold Policy supports a "hop" to the other ring if the station can properly manage the connection of the upper layers of the protocol stack to the active data path. The Hold Policy prevents a WRAP condition from occurring in the event of faults on a single ring. The network automatically switches the user data path to the surviving ring when the fault is detected and will remain there until the fault is corrected or a fault occurs on the second data ring. After a fault on the second ring, the network then operates with the standard reconfiguration policy as if the Hold Policy had never been used. Figures 4b and 4c illustrate the conditions for faults resulting the data path switching to the second ring and isolation (even with the Hold Policy enabled) for a six station ring. Isolation is a condition that is the result of segmentation of a ring based network such that the stations of the network are broken into multiple fully functional networks. As discussed later, when the Hold Policy is used and data is maintained on a single ring, a mechanism outside of the FDDI specification is necessary to properly control the association of the LLC with the ac-
Chapter 5: Analysis of the Hold Policy

In theory, the Hold Policy is capable of increasing the survivability of a network by allowing multiple faults on the same ring. However, there are some problems which are created when the Hold Policy is used. The problems include disrupting the hold state when adding or removing stations, loss of link integrity checking, address resolution, and path management. Each of these problems determine the usefulness of the reconfiguration mechanism. The two primary problems of concern for survivability are loss of hold after any problem no matter how minor in the surviving data path and the loss of the effect of the Link Error Monitor (LEM) flag.

5.1 Loss of Hold Due to a Transient on the Surviving Data Path

The simplicity of the mechanism controlling the Hold Policy makes it difficult to handle network reconfiguration while holding on one ring. With the current policy, if the ring is broken while holding on a particular data path, the ring will completely reconfigure to a WRAP state. During the normal operation of a ring, events such as station insertion, station removal and power glitches occur periodically. The formentioned events will prevent the Hold Policy from providing any added benefits to the network reconfiguration capabilities.

Station insertion and removal on a FDDI trunk ring while in the hold state causes the ring to wrap since both rings are momentarily broken. For a system which may have nodes entering and leaving a ring frequently, the normal operation of insertion and deinsertion would simply prevent the Hold Policy from having any beneficial effects on the operation of the network. The lack of the ability of a network to maintain hold on a ring after insertion or removal of stations is a major concern for networks which operate in hostile environments where any one event which leads to damage may cause effects on a number of different components. Bypass jitter while holding on a ring will break the hold state of the ring and is a major concern after a heavy shock. The added cost of the hardware necessary to support the Hold policy may be greater than the benefits if the policy is not enhanced in some way to permit momentary interrupts on the surviving ring as well as to allow insertion and removal of stations. This implies changes to the FDDI SMT specifications which would be difficult to achieve at this stage of FDDI development.
5.2 Link Error Monitor Problems

The actual algorithm for the Hold Policy is contained within two state machines of the SMT specification. The first place is in the ECM state machine at EC(11) as shown in Figure 5. When the ECM state machine first moves to the EC1:IN state, if the ring hold policy is used, the station will make transition EC(11a) if both the primary and secondary MACs are operational and the CFM machine is in the "Thru" state. If a station joins a ring and both the primary and secondary MACs become active (PM:NO-Flag = 0, SM:NO-Flag = 0) and the station goes into a Thru_AB state, the hold mechanism will then clear the RE_Flag (RE_Flag = 0) if it has not been cleared previously. The result will be to disable reconfiguration when faults occur on a single ring.

The second place where the Hold Policy is controlled is in the PCM state machine PC(81). The RE_Flag from the ECM state machine controls the transition back to the BREAK state from the ACTIVE state through transition PC(81) as shown in Figure 6. The effect of the RE_Flag is to prevent the condition (Break_Required | LEM_Fail | TNE>NS_MAX) from causing a transition to the BREAK state. Note that the RE_Flag will be a logical 0 when the Hold policy is used and both the primary and secondary rings are active.

The Break_Required condition is met if quiet symbols are received indicating that the ring is physically broken or the upstream neighbor is performing a link confidence test. The LEM_Fail will cause the break in the case that the link error monitor detects a faulty link due to excessive errors between two stations. The final condition is that TNE>NS_MAX which indicates that a burst of noise has disrupted a connection for a period of time which exceeds two frames.

The primary problem is in the use of the LEM_Flag in controlling the PC(81) transition. The LEM_Flag is used as an indicator of possible problems on a link and is controlled from the Link Error Monitor. This monitor continuously checks that the receiving links of the station operate within specified thresholds for errors. In the event that a link exceeds the error threshold (i.e. bent fiber or dirty connectors) the monitor will set the LEM_Flag. In normal operations this would result in reconfiguration (i.e. WRAP) and the link would be isolated. However, when the hold policy is in use, the LEM_Flag is prevented from being used until reconfiguration is enabled (i.e. RE_Flag set). The result is that links will be allowed to exceed the LEM threshold without being detected when the Hold Policy is active. Since the bad link is in the path of all stations, the number of retransmissions could prevent real time systems from operating effectively. Also, when connectionless operations are used to transfer data (i.e. at the Transport layer), large amounts of data could be lost without detection. The key point here is that this problem only exists when the Hold policy is used.

This problem will require one of two solutions. The first solution would be for the ANSI X3T9.5 committee to develop a method for dealing with the LEM_Flag while the Hold Policy is in use and is controlled from the Link Error Monitor. Since the hold policy acts as a global network policy and is not controllable by a single station, the latter of the solutions would be the most likely and logical method. A possible means of controlling this would be to place a management protocol above the SMT entity which would control which MAC the LLC would associate with depending on the status of the LEM_Flag. A more thorough explanation of this management entity is provided in reference [7].

5.3 Address Resolution Problems when using Dual-MACS

The reconfiguration scheme must be analyzed from the perspective of the full stack of protocols used. The use of two MAC entities, as previously described causes additional complexity for data transfers where a binding is dynamically reached to associate a MAC address with a Network Layer address. This dynamic address resolution
allows the placement of a fixed MAC level address in a hardware module (typically needed to support initial software loading across the network) which is dynamically resolved to a Network Layer address when needed. This permits changes in hardware modules (i.e. replacement or even swapping) from affecting the data communication users or higher level protocols. Examples of protocols that perform this function are the ARP protocol [9] in the Internet protocol family and the ES-IS Routing Exchange protocol [8] in the ISO/OSI protocol family. Implementations of such protocols utilize a cache (or data base) maintained at each station of all resolved Network/MAC addresses to which this station is communicating with. This cache is used for determining the destination address for MAC packets sent. Timers are typically used to automatically exchange "Hello" packets which keep these caches updated.

The ring hold reconfiguration approach uses two MACs to support a "hop" operation as previously described and is affected by the address resolution protocol due to the fact that the cache will contain the wrong MAC address right after a "hop". A timer based address resolution protocol will automatically correct this; however, the typical timer settings used may cause a of blockage of communications for a period of time that may be measured in minutes. This is a major problem for real-time systems where reconfiguration operations are needed in under a second.

In the development of the SAFENET draft, a number of methods were considered to support address resolution immediately following a hop: (1) Fixed relationship between the MAC addresses within a station; (2) Automatic change of the MAC address cache entries following a hop; (3) Shortening the time value used by the timers to send the "Hello" packets and (4) Changing the address resolution protocol. The SAFENET draft calls out a combination of the first three methods. The approach utilizes the address resolution protocol as the final authority for the contents of the cache but in the interval between a "hop" and the timers causing the exchange of "Hello" packets, the destination MAC addresses for stations on the ring are changed in the cache in a uniform way. The analysis indicated that this will allow communications to be maintained very quickly after wrap but did require customized features within the FDDI SMT Protocol and the address resolution protocol. A simple shortening of the timer intervals to under a second would have greatly increased the background traffic which was a concern in general but particularly after a "hop" operation where it is expected that a large amount of data may be queued up for transfer. The last method, changing of the address resolution protocol, while the most direct means to solve this problem was viewed as not being viable since the reconfiguration goals sought were beyond today's commercial practice and thus there existed no potential for changes to current standards.

5.4 LLC to MAC Association

With the addition of a second MAC to support the Hold Policy comes a new problem with determining which MAC to use for active data transmission and reception. There must be some mechanism to control the association of the LLC entity to the MACs. If the LLC is allowed to receive data from both MACs when the network wraps due to faults on both rings, each station receives broadcast and group addressed packets twice. To prevent this, the LLC must receive data from one and only one MAC. The mechanism for determining the association is not specified in any standard. The SAFENET draft supplies a simple state machine between the LLC and MAC entities which accomplishes consistent association.

6 Additional Reconfiguration Options

When the Navy first started looking at FDDI as a viable network protocol the industry was relatively new. Since then, the FDDI standard has progressed beyond the current specifications of the Navy. FDDI has always been a topology of a ring of trees, but until recently, the specification for the tree portion of the topology has been vague. Recent work in the ANSI X3T9.5 committee has resulted in specifications for the operation of concentrators which control the trees on a FDDI ring. This progress may provide the survivability that the Navy is looking for in tactical networks and further investigation into this topic is required.

The use of concentrators may ease the problems caused by optical bypasses by directly connecting stations to one or two concentrators. Any number of stations in the FDDI tree could be powered down and the network would still function. In general, the concentrators would not be powered down unless a major problem exists and optical bypasses could still be used on the trunk ring to interconnect concentrators without requiring a large number of individual stations to be powered up. Methods of attaching to two concentrators (dual homing) are also being developed which offer great potential benefits.

7 Conclusions

FDDI, with its Wrap mechanism built into every node that is attached to a trunk ring, is the first LAN standard which incorporates a reconfiguration mechanism into its protocol specification. This paper has provided a discussion on optional techniques for use on FDDI trunk rings to gain additional reconfiguration capabilities which are aimed at surviving multiple faults without segmenting into multiple independent rings. Such segmentation is used only as a last resort. In addition to the techniques discussed here, methods are being developed to utilize FDDI concentrators for survivability and availability enhancements. It is believed that the techniques described
here may be used in conjunction with concentrators to build interconnected systems more capable than those built with just one of these techniques alone.

One issue to be considered when developing a specification for systems is the use of options provided by a commercial standard. A number of vendors have integrated circuit implementations of much of the FDDI specifications and the requirement of a particular option within a standard may well eliminate certain products and thus limit implementation alternatives. The same is true for board-level and software products. Specifications may tie a system to an obsolete product if cited options are not included in future releases of the products due to lack of commercial support.

The Hold Policy approach discussed in this paper must be controlled by specific implementation guidelines in order to fully gain the benefits and justify the added cost and complexity of the system specifications. The cable plant must be partitioned into separate cables for each ring and no transients can occur on the surviving ring once the Hold Policy activates data transfer on a single surviving ring. Also, any implementation planning to use this technique needs to study how the issues of the Link Error Monitor, Dual-MAC Address Resolution and LLC to MAC Association will be handled.

8 Acknowledgments

The authors would like to thank the SAFENET committee for their participation in this project and particularly Ed Hotard of Martin Marietta for his significant contributions and comments on this paper.

9 References