DP83231,DP83241,DP83251,DP83255

AN-726 Station Management Simplified

Literature Number: SNOA195

Station Management Simplified

National Semiconductor
Application Note 726
My Le
December 1990

INTRODUCTION

One of the key areas in the FDDI standardization process has been the work on Station Management (SMT). The SMT document provides the guidelines and protocols which can be used to manage an FDDI network.

To ensure interoperability in a multi-vendor environment, some of the protocols described in the SMT document are mandatory. On the other hand, to facilitate the diverse network environments envisioned for FDDI, many protocols described are optional. Thus the users need to determine the SMT protocols to be implemented based on their application and configuration requirements.

This application note provides an introduction to FDDI Station Management with the assumption that the reader is familiar with the MAC, PHY, and PMD portions of the FDDI protocol.

The following topics are included in this paper:

- Station Management Requirements
- Structure of FDDI Station Management
- Basic SMT frame work to manage an FDDI network
- Optional management protocols based on configurations and applications
- SMT features provided by the National's DP83200 FDDI chip set

1.0 SMT Requirements

Before determining the SMT requirements for FDDI, let's define the major types of users of the network. Based on the requirements of the users, we can then determine the functions required by SMT.

1.1 TYPES OF USERS

Users can be divided into two main groups: End-Users and Network Administrators.

The End-Users are mainly interested in the services which the network provides; thus, SMT operations on the network should appear transparent to the End-Users.

The second major type of user in an FDDI network is the Network Administrators. While the End-Users would like to know as little as possible about the network, the Network Administrator's goal is to gather as much information about the network and its attachments as possible; thus SMT should be designed to allow the Network Administrators to control the network in a manner that is unobtrusive to the End-Users.

End-Users

The main requirements of the network by End-Users are:

• Network Services Reliability

One of the top requirements from the End-Users is the reliability of the network. The network should remain up and running with the probability of an error occurring as infrequently as possible.

When an error does occur, it should be isolated while the rest of the network that is free from the error should continue to operate. And finally, the error should be detected and removed from the network in a deterministic fashion as quickly as possible.

Thus, SMT needs to provide extensive and complete Fault Detection and Recovery procedures to satisfy the requirement of network's reliability.

• Access to All Authorized Networked Resources

SMT can be used to provide the mechanism for the End-Users to obtain the services available on the network. This service is useful, especially in a multi-vendor environment, to guarantee that all stations can receive the same types of network services regardless of their particular implementations.

An example of the services provided by the FDDI network is Synchronous Bandwidth Allocation. Using this service, stations can then obtain part of the bandwidth to transmit synchronous data.

• Plug-and-Play

Connection to a network should be made as simple as possible such that the End-Users can plug into the network without the need for complicated instructions or the possibility of bringing down the network by mistake.

This requirement is especially important in a large network such as FDDI where a large number of stations can potentially be connected, disconnected, or moved at any given time.

To satisfy this requirement, SMT needs to provide a comprehensive connection management procedure to allow stations to be connected quickly and correctly to the network.

Network Administrators

The main requirements of the network by Network Administrators are:

• Ability to Gather Information

One of the key functions of Network Administrators is to monitor the status of the network and the attached stations. To achieve this goal, the Network Administrators must have the capability of requesting and receiving information from stations on the network.

From the information gathered, the Network Administrators can then determine the status of the network and invoke any recovery mechanisms if necessary.

To meet this requirement, SMT needs to provide a monitoring procedure where the Network Administrator can gather information frequently and accurately.

• Standardized Management Services

In an open network environment where the Network Administrators have to control equipment from a large number of vendors, there is a need for standardized management services to allow the Network Administrators to communicate with any station on the network regardless of its implementation.

RRD-B30M75/Printed in U. S. A.

The standardized management services also allow the Network Administrators to interpret the information received from the stations.

• Flexible Network Configuration

Networks can be designed in many configurations depending on many factors such as applications used, building structure, etc. A network that can be configured in many different forms gives the Network Administrators the flexibility to design the network based on their own requirements and constraints.

FDDI Station Management provides the Connection Management procedure which allows the network to be connected into many different configurations (e.g., dual ring of trees, single tree, dual ring, etc.).

• Ability to Manage the Network Remotely

It is desirable for the Network Administrators to monitor activities on the network or trouble-shoot problems from a central location. It is also desirable to down-load information without physically being at the stations.

To provide these types of services, SMT needs the capabilities to control the remote stations and order them to perform certain operations.

1.2 SMT FUNCTIONS

Based on the types of users on an FDDI network and their applications as described above, a list of the SMT requirements can be drawn up as follows:

- Fault management for high network availability
- Reliable error detection and recovery management
- Access to networked resources
- Fast and reliable connection management procedure
- Management for multi-vendor networks
- Access to individual station information
- Flexible configuration

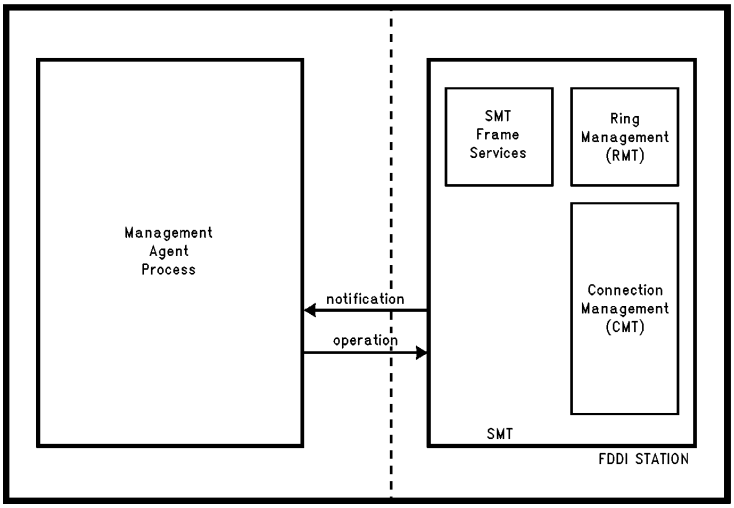
2.0 SMT Structure

SMT is the layer management service for FDDI networks which covers the Physical (PHY) and Media Access Control (MAC) Layers. SMT serves two main purposes in an FDDI network:

1. To collect information to report to the Management Agent Process which is responsible for the management of the entire station (above the PHY and MAC Layers), and
2. To manage stations on the network by starting and maintaining the PHY and MAC Layers.

SMT is divided into three main groups: Connection Management, Ring Management, and SMT Frame Services. The functions of these entities are described followed by a more detailed discussion on each.

Figure 1 shows the overall SMT Architectural model.



TL/F/11080–1

FIGURE 1. Station Management (SMT) Architectural Model

2.1 Connection Management

Connection Management (CMT) is the management entity in SMT that is responsible for the Ports (a Port is a PHY and PMD pair) and their interconnections to their neighboring Ports. It is also responsible for the configuration of MACs and PHYs within a station.

CMT's functions include the following:

- Establish and initialize physical connections
- Control station configuration
- Detect Physical Layer faults

The CMT entity is further divided into three sub-entities: Entity Coordination Management, Physical Connection Management, and Configuration Control Management.

Entity Coordination Management

The Entity Connection Management (ECM) indicates when the media is available (i.e. when signals can be transmitted and received). It is also used to coordinate activities of other entities within CMT and RMT.

There is one ECM entity per Station or Concentrator.

Physical Connection Management

The Physical Connection Management (PCM) initializes the connection of Ports and manages the Signaling Sequence between each physical connection.

The PCM uses the Line States available in the PHY to perform the Signaling Sequence.

There is one PCM entity for each Port.

Configuration Control Management

The Configuration Control Management (CCM) controls the interconnection of PHYs and MACs within a node to configure one of the following node types:

- Single Attach Station (SAS)
- Dual Attach Station (DAS)
- Single Attach Concentrator (SAC)
- Dual Attach Concentrator (DAC)

There is one CCM entity per Port.

2.2 Ring Management

Ring Management (RMT) is the entity in SMT that is responsible for the MACs within a station.

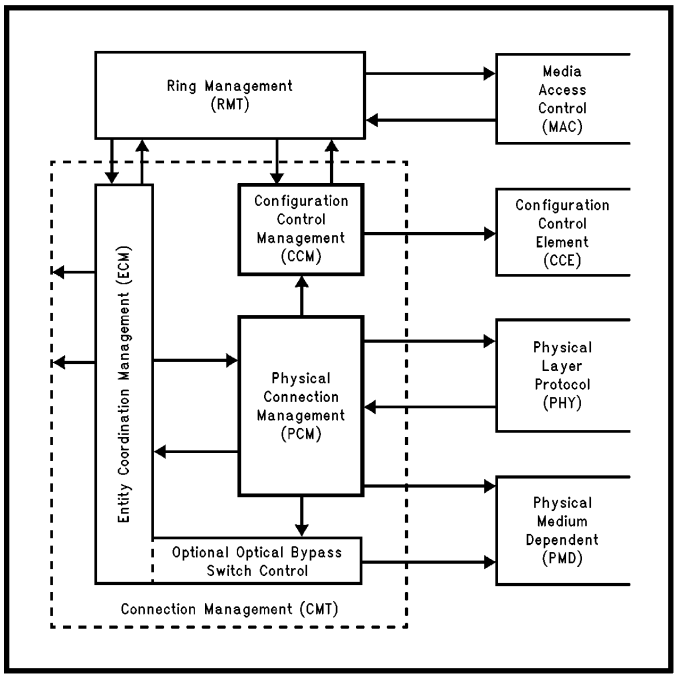
RMT's functions include the following:

- Notify station of MAC availability
- Detect logical MAC Layer faults

The RMT entity receives status information from the MAC and the Configuration Control Management (CCM) entity. The information is then reported to the higher-level management entity.

There is one RMT entity for each MAC in a Station or Concentrator.

Figure 2 shows the internal structure of the CMT and RMT entities.



TL/F/11080–2

FIGURE 2. RMT and CMT Entities

2.3 Frame Services

Frame Services is the management entity in SMT that is responsible for providing a number of frames that may be used to gather information and control the stations attached to the network. These frames are used in SMT protocols which collect information for higher-level management entities.

Frame Services are used by the Management Agent Process to:

- Gather statistics
- Detect, isolate, and resolve network failures
- Tune performance
- Change topology

3.0 Basic SMT Framework

All entities within SMT, Connection Management, Ring Management, and Frame Services, are operated based upon the following inputs:

- Signals from higher level management
- Internal conditions triggered by the expiration of timers
- Signals received from other stations on the network

Since SMT is considered as an intelligent entity, the higher level management does not need to control every level of operation within SMT. Rather, SMT will perform the necessary procedures and protocols to accomplish a task requested when the higher layer management entities set the appropriate signals (Connect, Disconnect, Reset, etc.).

3.1 CONNECTION MANAGEMENT

CMT controls the Physical Layer (PHY and PMD) and the Configuraiton Control Element which connects the MACs and PHYs within a station or concentrator.

The operation of CMT is based upon the requests from SMT which in turn come from a higher level of management. The requests used to control CMT are:

- Connect Request: this request is used to signal the Physical Layer to connect to or disconnect from the network (signals Connect and Disconnect).
- Control Request: this request is used to signal the CMT to perform certain operations or to report status.

CMT communicates with SMT via Status Indication which is used to report CMT status changes.

Entity Coordination Management

The ECM is initialized when the CMT receives a Connect Control Request from SMT.

The services provided by the ECM Entity are:

- Connects the PMD to the network when CMT is initialized:
  - — Allows the Transmitter and Receiver to begin to transmit and to receive.
  - — Once the Fiber Optic Transmitter and Receiver are ready, a signal is set to initialize the PCM.
- Starts the Trace process to localize a Stuck Beacon condition based on the Trace_Prop signal from the Ring Management or Physical Connection Management entity.
  - — After the ring is stuck in the Beacon state for a period of time ($\geq$ 8.0 seconds), a signal is set to begin the Trace process.
  - — ECM performs the Trace function by invoking the PCM to transmit the appropriate Line States.
- Disconnects the PMD from the network
- A Path Test function is used to test all the components and paths within a node. Since the test occurs entirely within a node and cannot be verified, it is considered an implementation dependent issue and is not specified by the Standard.

  The Path Test is used to ensure that the node will operate correctly once it joins the ring. It is also used to determine if the node causes errors on the ring.

  For example a Path Test can include the following steps:
  - Test all accessible data paths within the node
  - Perform loopback testing of the PHY as close as possible to the PMD interface
  - Confirm parameters provided to the MAC: addresses, timer values, etc.
  - The MAC recovery process for this node including the resolution of the Beacon and Claim Processes

Physical Connection Management

PCM is initialized by the PC_Start signal from the ECM.

PCM provides the following services:

- Initializes a physical connection. The physical connection procedure is performed at the PHY Layer as follows:
  - — Determines that a neighboring PHY exists
  - — Determines that the neighboring PHY has the correct PC_Type to establish a legal connection between the two Ports. [In a typical network configuration, there are two types of legal connections: A to B (Dual Attach Stations on dual rings) and M to S (Single Attach Station connected to a Concentrator).]
- Runs the Link Confidence Test. The Link Confidence Test is used to determine if the link quality is adequate for ring operation. Its aim is to detect major link quality problems, not to determine the exact Link Error Rate.

  The Link Confidence Test is performed in the PCM State Machine before the link is allowed to join the ring. A minimum Link Confidence test requires the transmission of Idle symbols for a period of 50.0 ms providing that the link has not had any recent link quality problem. Errors that occur during the testing period are recorded. If the number of errors recorded exceeds the acceptable error rate, the test fails. Otherwise, the link is considered to have passed the Link Confidence test.

  The result of the Link Confidence Test is reported to higher level management. If the link fails the test, it will continue to be tested until the test is passed or until higher level management disconnects the link.

  Once the Link Confidence test has been completed successfully, the link is ready to be included in the network. The PCM then signals the CCM to connect the appropriate MACs and PHYs together within a station.

  The Link Error Monitor (LEM) is used to examine the link error rate of an active link. The LEM function complements the initial Link Confidence test to monitor the link quality once it has joined the ring.

  LEM is performed by SMT using the facilities available in the PHY.

Link Error Events are counted to produce the LEM__CT count. A Threshold test is used to compare the current Link Error Rate with the cutoff and alarm Link Error Rate thresholds.

Once the LER reaches the alarm LER threshold, SMT reports the status to higher level management. If the LER is equal to or greater than the cutoff LER thresholds, the link is automatically removed from the ring and this event is reported to higher level management.

- Performs the Trace function.

  Upon the reception of signal PC__Trace from ECM, PCM transmits the appropriate Line States required by the Trace function.

  The Trace function provides a recovery mechanism for Stuck Beacon conditions on the FDDI ring. Whereas PCM is designed to recover from most physical faults that occur between two nodes, the Trace function is intended to provide recovery from a Stuck Beacon condition which cannot be localized to a single link.

  The Trace function causes all stations and concentrators in the suspected fault domain to leave the ring and complete a Path test, so that the fault may be localized. The fault domain is defined as the area between the Beaconing MAC and its nearest upstream neighbor MAC.

  The Trace function is performed as follows:

  - When a station enters the Beacon State, a timer is reset. If the station is still in the Beacon state when the timer expires, a Stuck Beaconing condition has occurred and the RMT sets the Trace__Prop signal to the ECM to initialize the Trace function.
    - — The Trace function starts at the node with the Beaconing MAC and traverses to the nearest upstream MAC.
    - — The ECM controls the configuration information and sets the PC__Trace signal to the appropriate PCM. When a PCM receives a PC__Trace signal, it transitions to the Trace state to transmit a special line state that indicates Trace.
    - — The Port at the other end of the link receives the ''Trace'' Line State and will set the Trace__Prop flag to indicate that the Trace function is to be propagated upstream.
    - — When the Trace Line State arrives at a Port that is connected to the input of a MAC, the Trace has been completed.

      The node with the MAC that receives the Trace removes itself from the ring from Path Test.
    - — The removal of this node causes the node downstream from it to remove itself also.

      Thus, all nodes in the Trace domain will eventually remove themselves from the ring to perform Path Tests. This process should take less than the Trace__Max timer value (7 seconds).

    If the Trace function has not been completed within the Trace__Max time, the process has failed and manual intervention is required.

    Once the Trace function has been completed, it will indicate the result to ECM.
  - Supports Maintenance.

    In the Maintenance state, the PCM can transmit any sequence of symbols. This feature is useful to ensure that the PHY Transmitter can transmit all the symbols in the FDDI Code. It is also used to force the other end of the connection into a particular state manually without going through the Connection Sequences.

Configuration Control Management

The CCM is initialized by the CF__Join signal from the PCM.

The services provided by the CCM Entity are:

- Inserts Single Attachment Station or Concentrator to the Primary Path.
- Connects the MAC of Dual Attachment Station or Concentrator with a Single MAC to the Primary Path.

  In this configuration, all Dual Attach Stations with one MAC are connected to the Primary Ring. Only Dual Attach Stations with two MACs can transmit and receive frames on both the Primary and Secondary Rings.

  Single Attach Stations are connected to the Primary ring as the default configuration.
- Performs the Scrub function.

  The Scrub function is used to remove PDUs sourced by MACs that no longer form part of the same token path. These MACs may have been removed from the token path internally within its node or due to a network topology change. It is controlled by the CEM entity.

  The Scrub function removes left over PDUs after a reconfiguration to ensure that all PDUs on the ring have been created since the last reconfiguration.

  The Scrub function may be performed by using one of several mechanisms listed below.
  - — Transmit Beacon or Claim frames for a sufficient time while the input to the MAC is blocked (stripping old frames while transmitting Beacon or Claim frames)
  - — Transmit Idle symbols for a sufficient time while discarding input stream received at the PHY. This method may be used for a node that does not have a MAC after reconfiguration.
  - — Frames can also be stripped by the node that is performing the Scrub function.

3.2 RING MANAGEMENT

RMT manages the basic information and condition of each MAC. The operation of RMT is based upon the control request from SMT, which in turn comes from the higher level of management. This request is used to signal RMT to reset, to change the basic information in the MAC, or to report its status. RMT is also responsible for initiating fault recovery actions to recover the ring.

RMT communicates with SMT via the Status Indication which is used to report its status changes.

Services provided by RMT are:

- Identification of a Stuck Beacon condition

  If the ring remains in the Beaconing state for a long time ($\geq$ 8.0 seconds), the Stuck Beacon condition has occurred. RMT will report this error condition to higher level management as well as starting a new error recovery mechanism.

  RMT uses a timer (T_Stuck) to keep track of the Struck Beacon condition.

- Initiation of the Trace function

  Once the ring has been identified to be in the Stuck Beacon condition, RMT starts the Trace function by setting the Trace_Prop signal to ECM.

- Notification of MAC availability

  After the CCM sets the RM_Join signal to indicate that the MAC is connected to the appropriate PHY in a station (or concentrator), the RMT can then set the MAC_Available signal to higher level management to indicate that the MAC is ready to transmit and receive data.

- Detection of Duplicate Addresses

  By observing the order in which Beacon and Claim frames are received at the MAC, RMT can detect Duplicate Addresses which can prevent the ring from becoming operational.

  Upon detecting this condition, RMT will notify higher level management of the condition. It will also take actions to resolve the Duplicate Address problem.

- Resolution of Duplicate Address Problem

  One of three possible solutions can be taken by RMT to eliminate the Duplicate Address problem:

  1. Change the MAC's address to a unique universal address
  2. Change the bidding time to guarantee that this station will lose the Claim Process
  3. Remove the station from the ring

3.3 FRAME SERVICES

A number of frames are specified as SMT frames. These frames are used to gather information and control the operation of the stations on the network. There are four types of mandatory SMT frames:

- Neighbor Information Frame
- Resource Allocation Frame
- Request Denied Frame
- Status Report Frame

Neighbor Information Frame

A Neighbor Information Frame (NIF) is used by a station for periodic announcement of its basic operating information. Based on the Upstream Neighbor Address provided in NIF frames, a station can then build a ring map of the stations' locations and their connections to other stations.

There are three types of NIFs: Announcement, Request, and Response.

• Announcement

A NIF Announcement frame is broadcast to the entire ring.

A station can choose to transmit a NIF Announcement or NIF Request. If a NIF Announcement is to be transmitted, it will be sent every 30 seconds when the ring is operational and under zero load conditions.

• Request

A NIF Request is sent to a station, a group of stations, or the entire ring. The NIF Request announces the station's information while requesting that the corresponding station(s) respond with a NIF Response.

If an NIF Request is to be transmitted, it will be sent every 30 seconds when the ring is operational, under zero load conditions.

• Response

A NIF Response is sent in response to a NIF Request.

Upon receiving a NIF Request, a station is required to send a NIF Response within 30 seconds if the ring is operational, under zero load conditions.

In addition to the Upstream Neighbor Address, the NIF Response frame also provides the Downstream Neighbor Address, and the mechanism to detect Duplicate Addresses.

Resource Allocation Frame

A Resource Allocation Frame (RAF) is defined to support a variety of network policies for allocation of resources. At this point, only the Synchronous Bandwidth is identified as the only resource supported by the Resource Allocation Frames. However, the protocol can also be used to support other types of resource allocation which have yet to be specified in the Standard.

Request Denied Frame

A Request Denied Frame (RDF) is used to respond to optional frames that the station does not support. It is also used to respond to an SMT frame with a Version ID that this station does not support.

Status Report Frame

The Status Report Frame (SRF) is used to periodically announce the station's status which may be of interest to the Network Administrator.

Two types of information are included in the SRF: Conditions and Events. Conditions include the station state which may be of interest to a network manager as long as the condition remains asserted. Events are instantaneous occurrences which are of interest to a network manager.

4.0 Optional Protocols

Aside from the mandatory functions listed in Section 2.0, FDDI SMT also provides many optional protocols that can be implemented in addition to the mandatory ones.

4.1 CONNECTION MANAGEMENT

Entity Coordination Management

ECM has two optional features, the Optical Bypass Switch Control and Hold Policy.

• Optical Bypass Option

The Optical Bypass is used to allow a Dual Attachment Station or Concentrator to be inserted and deinserted from a dual ring without disrupting the operation of the ring.

If the Optical Bypass Option is available, the ECM allows for the switching time of the optical bypass switch during the Insertion process. It also allows time for the optical bypass switch to deinsert during the Deinsertion Process.

• Hold Policy Option

When the Hold Policy is invoked, it prevents the dual rings from wrapping when a fault occurs on one of the two rings. The Hold Policy may be used in Dual Attachment Stations and Concentrators.

The Hold Policy is useful in preventing the disruption of a ring when an error occurs on the other ring of the dual rings (disruption occurs when the ring attempts to wrap).

Physical Connection Management

PCM has the following two optional Features

• Physical Connection

In a normal dual ring of trees structure, there are two types of physical connections between two ports: A–B (A port to B port) and M–S (Master port to Slave port). In addition to these two connections, other connections can also be acceptable as legal:

- A port to A port (A–A)
- B port to B port (B–B)
- A port to Master port (A–M)
- B port to Master port (B–M)
- Slave port to Slave port (S–S)

The A–A and B–B connections may be used when two Dual Attachment Stations are connected together to form a ringlet (a dual ring with two stations).

The A–M and B–M connections may be used when a Dual Attachment Station is used as two Single Attachment Station. In this case, the station can only be connected to the ring via a Concentrator. This scenario is called Dual-Homing.

The S–S connection may be used to connect two Single Attachment Stations together to form a link. The two stations thus form a single ring.

Although these connections are considered legal, higher level management needs to be notified so that the link can then be rejected.

• Link Confidence Test

Aside from the minimum Link Confidence Test described in Section 3.4, other types of Link Confidence tests can be performed.

The two PHYs of the link need to agree beforehand which type of Link Confidence test is to be carried out. This information is exchanged via a bit in the PCM Signaling Sequence.

Other Link Confidence tests to be considered include the following:

- Transmitting PDUs and counting link errors. Errors are detected and counted at the PHY.

  This Link Confidence test requires at least one MAC connected to one of the two PHYs.
- Transmitting PDUs and counting Frame Check Sequence errors. Errors are detected and counted as frame errors at the MAC.

  This Link Confidence test requires at least one MAC connected to one of the two PHYs.
- Looping back symbols received from the other end of a connection and counting link errors on reception. Errors are detected and counted at the MAC.

  This Link Confidence test is performed at the PHY layer.

The length of the Link Confidence Test can be:

- Short (50.0 ms)
- Medium (500.0 ms)
- Long (5.0 sec.)
- Extended (no maximum time specified)

The length of the Link Confidence test is indicated by two bits of the PCM Signaling Sequence.

Configuration Control Management

Aside from the Primary Path, there are two other optional paths available in CCM: Secondary and Local.

- A PHY or a MAC can be connected to the Local Path. While connected to the Local Path, these entities are removed from the ring and can be used to perform local testing.
- A Single Attachment Station can initially be connected to the Secondary Path. Single Attach Stations can then choose to transmit and receive frames on either the Primary or Secondary ring depending upon the initial connection.
- The MAC of a Dual Attachment Station with a Single MAC can also optionally be connected to the Secondary Path. Stations with one MAC can then choose to transmit and receive frames on either the Primary or Secondary ring.

4.2 FRAME SERVICES

The following SMT frames are provided by the Frame Services to gather status and control the nodes on the ring:

- Station Information Frames
- Echo Frames
- Extended Service Frames
- Status Report Frames
- Parameter Management Frames

Station Information Frame (SIF)

Station Information Frames (SIFs) are used to request and provide, in response, a station's configuration and operating information. There are two classes of SIFs: Configuration and Operation.

• Configuration SIF

A station can request a station, a group of stations, or all stations on the ring to respond with its (their) configuration information using the SIF Configuration Request. The transmission of these Request frames is optional.

A station is required to respond to SIF Configuration Request frames with a SIF Configuration Response frame within 30 seconds of receiving a Request frame, under zero load conditions. Stations can also deny the request by sending back a Request Denied Frame.

The SIF Configuration Response provides the configuration structure of the node by describing the connections of the PHYs and MACs within the node. It is used to build the full ring map (both logical and physical).

• Operation SIF

A station can request a station, a group of stations, or all stations on the ring to respond with its (their) operation information using the SIF Operation Request. The transmission of these Request frames is optional.

A station is required to respond to SIF Operation Request frames with a SIF Operation Response frame within 30 seconds of receiving a Request frame, under zero load conditions.

The SIF Operation Response provides the operating parameters in a node; information such as timer values, counter values, etc. It is used to detect faults by monitoring the station's status and counter values.

Echo Frames

A station can request another station on the ring to re-transmit a test pattern using the Echo Request Frame (ECF). This test pattern is stored in the Information field of the Echo Request Frame.

Upon receiving the Echo Request Frame, the recipient builds an Echo Response Frame and sends it to the Request Frame's Source Address.

The Response Frame is required to be transmitted within 30 seconds after receiving the Request frame if the ring is operational and there is zero load. The recipient can also send a Request Denied Frame instead of the Response Frame.

Echo Frames can be used to test for data-sensitive network failures by placing the suspect data pattern in the Echo Information field. It can also confirm that a station's Port, MAC, and SMT are partially operational.

Extended Service Frame

The Extended Service Frame (ESF) can be used to test new SMT services that are intended for inclusion in later versions of the FDDI SMT document.

The structure of the ESF is defined by the owner of the Extended__Type.

Parameter Management Frames

The Parameter Management Frames (PMF) are used to get, change, add or remove parameters in a node. There are 4 classes of PMFs: PMF Get, PMF Change, PMF Add, and PMF Remove.

There are two types of frames for each class: Request and Response.

PMFs are transmitted with an optional authorization code to provide a type of security check.

PMF Get

A station can issue a PMF Get Request Frame to query the value of one or a group of attributes in the Management Information Base (MIB) of an individual, group, or all stations.

The receiving station can respond with the current value of the requested attributes. If the protocol is not supported, a station can transmit a Request Denied Frame in return.

PMF Change

A station can issue a PMF Change Request Frame to change the value of a single attribute in the Management Information Base of an individual, group, or all stations.

The receiving station can act to change the requested attribute. It can then respond with a PMF Change Response. A station could also transmit a Request Denied Frame in return.

PMF Add

A station can issue a PMF Add Request Frame to add a value of a single attribute in the Management Information Base of an individual, group, or all stations.

The receiving station can act to add the requested value. It can then respond with a PMF Add Response. A station could also transmit a Request Denied Frame in return.

PMF Remove

A station can issue a PMF Remove Request Frame to remove the value of a single attribute in the Management Information Base of an individual, a group, or all stations.

The receiving station can act to remove the requested value. It can then respond with a PMF Remove Response. The station could transmit a Request Denied Frame in return instead.

5.0 National's FDDI Chip Set

National's DP83200 FDDI Chip Set has been designed to provide maximum support to the Station Management functions. Both the PLAYER and BMAC devices have separate management interfaces via the Control Bus. Furthermore, each chip has many registers on-board to provide the information required by the different SMT entities.

5.1 PLAYER DEVICE

Connection Management

The Connection Management Entities (ECM, PCM, and CCM) can control the operation of the PMD and PHY using the registers available on the PLAYER Device.

• Entity Coordination Management

The user can control the operation of the PMD by setting or resetting bits 4 to 7 of the MODE Register.

• Physical Connection Management

The PCM Signaling Sequence can be implemented using the Current Transmit State Register and Current Receive State Register in the PLAYER device.

Line States can be transmitted by setting the appropriate bits in the Current Transmit State Register. Line States received can be monitored observing the Current Receive State Register.

Furthermore, a historical record of the Line States received is kept in the Receive Condition Registers. This information is useful for keeping track of the Signaling Sequence.

The Noise Threshold and Noise Prescale Threshold Registers are used to ensure that the noise conditions do not persist beyond the maximum tolerated level.

• Configuration Control Management

Using the Configuration Register, the CCM can control the connection of the PHYs and MACs in a node. Each PLAYER Device can be connected to the Primary Path, Secondary Path, and Local Path. In addition, it can also be connected to the PHY Invalid Bus where the PLAYER Device can continuously transmit PHY Invalid to the ring or indicate PHY Invalid to the entity it is connected to internally within the node (i.e., a BMAC Device or another PLAYER Device).

The PLAYER Device can be configured via the Configuration Register without external logic.

Link Error Monitor

SMT can use the following registers to perform the Link Error Monitor functions once the PLAYER Device is connected to the ring:

- Current Noise Count Register
- Current Noise Prescale Count Register
- Link Error Threshold Register

These registers enable the user to implement different methods of monitoring link errors according to their requirements.

Loopback

The PLAYER Device can be programmed to perform Internal or External Loopback. These Loopback operations are useful during Path Testing.

The Internal Loopback mode can be used to test the functionality of the PLAYER Device or to test the data path between the PLAYER and BMAC Devices.

The External Loopback mode can be used to test the functionality of the PLAYER Device and to test the data paths between the PLAYER Device, Clock Recovery Device, and BMAC Device. This mode is especially useful when the Path Test requires testing as close to the PMD as possible.

5.2 BMAC Device

The BMAC Device provides extensive ring and station statistics via the on-board Timer and Counter Registers. Furthermore, it can internally generate Claim and Beacon frames that are used in the FDDI MAC Protocol to detect errors.

Timers and Counters

Information can be provided to RMT and other SMT entities to represent the operating status of the node using the following Counters and Timers:

- Late Count Counter
- Frame Received Counter
- Error Isolated Counter
- Lost Frame Counter
- Frame Copied Counter
- Frame Not Copied Counter
- Frame Transmitted Counter
- Token Received Counter
- Ring Latency Counter
- Negotiated Target Rotation Timer
- Maximum Token Rotation Timer
- Valid Transmission Timer
- Asynchronous Priority Threshold

The information provided can then be transmitted to other stations on the ring in the Station Information Operation Response Frame and Status Report Frame.

Loopback

The BMAC Device can be programmed to perform loopback testing.

There are three Self-Test Paths:

- Internal to the BMAC Device
- Through the PLAYER Device(s)
- Through the CRD Device

These paths allow the user to perform Path Tests on the BMAC, PLAYER, and CRD Devices.

Stripping Protocol

A special stripping protocol can be invoked by asserting the STRIP signal (pin 13). The stripping protocol starts with the transmission of two My__Void frames at the end of a current service opportunity. The stripping will continue until a My__Void frame returns. The stripping protocol can be invoked when the initial token is issued after a successful Claim to remove all fragments and ownerless frames from the ring as required by the Scrub function of the Configuration Control Management entity.

Inhibit Recovery

By setting bit 3 of the Option Register, the MAC can be prevented from entering the Claim state.

This option is useful in allowing the ring to recover from the Duplicate Address scenario where two stations with the same address also have the winning Claim frames. By prohibiting one station to enter the Claim state, the other station can then win the Claim process thus allowing the ring to become operational.

Claim and Beacon Frames

The BMAC Device reports the reception of a Claim or Beacon frame by setting the appropriate bit in the Ring Event Latch Registers.

By keeping track of the received Claim and Beacon frames, the user can then determine if the Error Recovery process (Claim or Beacon) has succeeded or failed.

Duplicate Address Detection

Upon the detection of a Duplicate Address, the BMAC Device reports the incident by setting the appropriate bit in the Ring Event Latch Registers.

Duplicate Token Detection

Upon the detection of a Duplicate Token, the BMAC Device reports the incident by setting the appropriate bit in the Token and Timer Event Latch Register.

6.0 Summary

The Station Management (SMT) facilities, an essential part of an FDDI network, provide a rich set of tools to manage an FDDI network. As a summary, the Connection Management services of SMT manage the configuration of the station and the link between the station's Ports and their neighboring Ports; the Ring Management facilities provide control of the MACs of a station in the FDDI rings; the Frame Services provide a tool to manage the complete FDDI network, the services are the most flexible and extensive part of SMT.

The implementation of Station Management software can be rather complicated without adequate support from the hardware. As a result, the National Semiconductor Corporation DP83200 FDDI Chip Set integrated many essential functions on the chip set and provides maximum support to FDDI Station Management functions. The PLAYER Device and the BMAC Device support the Connection Management services and the Ring Management service respectively. The BSI Device provides separate Station Management channel and data frame channels for the maximum support of the SMT Frame Services. The invaluable Station Management features in the DP83200 Chip Set can shorten the Station Management software development cycle and provide higher reliability of the FDDI network.

National Semiconductor Corporation
2900 Semiconductor Drive
P.O. Box 58090
Santa Clara, CA 95052-8090
Tel: 1(800) 272-9959
TWX: (910) 339-9240

National Semiconductor GmbH
Livry-Gargan-Str. 10
D-82256 Fürstenfeldbruck
Germany
Tel: (81-41) 35-0
Telex: 527649
Fax: (81-41) 35-1

National Semiconductor Japan Ltd.
Sumitomo Chemical
Engineering Center
Bldg. 7F
1-7-1, Nakase, Mihama-Ku
Chiba-City,
Ciba Prefecture 261
Tel: (043) 299-2300
Fax: (043) 299-2500

National Semiconductor Hong Kong Ltd.
13th Floor, Straight Block,
Ocean Centre, 5 Canton Rd.
Tsimshatsui, Kowloon
Hong Kong
Tel: (852) 2737-1600
Fax: (852) 2736-9960

National Semiconductores Do Brazil Ltda.
Rue Deputado Lacorda Franco
120-3A
Sao Paulo-SP
Brazil 05418-000
Tel: (55-11) 212-5066
Telex: 391-1131931 NSBR BR
Fax: (55-11) 212-1181

National Semiconductor (Australia) Pty, Ltd.
Building 16
Business Park Drive
Monash Business Park
Nottinghill, Melbourne
Victoria 3168 Australia
Tel: (3) 558-9999
Fax: (3) 558-9998

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Audio	www.ti.com/audio	Communications and Telecom	www.ti.com/communications
Amplifiers	amplifier.ti.com	Computers and Peripherals	www.ti.com/computers
Data Converters	dataconverter.ti.com	Consumer Electronics	www.ti.com/consumer-apps
DLP® Products	www.dlp.com	Energy and Lighting	www.ti.com/energy
DSP	dsp.ti.com	Industrial	www.ti.com/industrial
Clocks and Timers	www.ti.com/clocks	Medical	www.ti.com/medical
Interface	interface.ti.com	Security	www.ti.com/security
Logic	logic.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Power Mgmt	power.ti.com	Transportation and Automotive	www.ti.com/automotive
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Mobile Processors	www.ti.com/omap		
Wireless Connectivity	www.ti.com/wirelessconnectivity		
	TI E2E Community Home Page		e2e.ti.com

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265