



## MMS Product Description Table of Contents

1	General.....	1
2	ICAO Compliance .....	1
3	Operating System Compatibility.....	1
4	Hardware Composition and Testing.....	2
5	Wide Area Network (WAN) and AMHS .....	3
	5.1 - Partial-mesh Considerations.....	4
	5.2 SVC, PVC and Bandwidth Considerations.....	5
	5.3 AMHS and ATN Considerations .....	5
	5.4 Protocol Translation.....	7
	5.5 Mobile User and Wireless Considerations.....	7
	5.6 VSAT Considerations.....	7
6	AFTN WAN as General Purpose CAA Network .....	8
7	Software License .....	8
8	Capacity .....	8
9	Reliability.....	9
10	Resilience .....	10
11	Long Term Cost of Ownership .....	10
12	Connectivity and Scalability.....	11
13	Maintainability .....	12
14	Communication Interfaces .....	13
15	Error Checking and Control.....	14
16	End-to-End Loopback Checks and Confirmation Messages .....	15
17	Automatic Repeat Request and Response .....	15
18	User Interface .....	15
19	Predetermined Address Lists (Collectives and broadcast messages).....	16
20	Configuration Control .....	16
21	Functional Assignments and Automatic Reconfiguration.....	16
22	Routing Control .....	17
23	Alternate Routing .....	17
24	Load Balancing.....	17
25	Message Retrieval Functions .....	18
26	Message Archiving and Storage .....	19
27	Built-In Text Editor.....	19
28	Message Validation and Envelope Generation.....	19
29	Address Book .....	20
30	Oversize Message Handling .....	20

31	On-Line Statistics and Reports .....	20
32	System Monitoring and Control .....	21
33	System Clock .....	21
34	Built-In and Definable Message Templates .....	21
35	Deferred Messages .....	22
36	Keyboard Macro Facility.....	22
37	Automated Dial Backup Configuration for Concentrator Sites .....	22
38	Automated Dial-Up Message Service for End-Users .....	23
39	Unattended Operation Parameter .....	23
40	Contingency System Option .....	24
41	NOTAM Handling Option .....	24

# MMS - Multi-protocol Message System

## 1 General

The Multi-protocol Message System (**MMS**) offered by Digital Resources Inc. (**DRI**) is a general purpose store-and-forward message switching system that maximizes the advantages of modern network techniques. The MMS is completely parameterized, and can implement networks ranging from the obsolete point-to-point configuration, up through the most up-to-date wide area network (**WAN**) applications. It can be implemented for various types of message switching applications, including the ICAO defined AFTN, AMHS, ATN, the ITU defined F.31 networks, WMO, etc. The MMS is designed to maximize the economic and hardware support advantages of a personal computer (**PC**) based WAN approach, over the point-to-point design. The MMS takes full advantage of continually decreasing server and PC costs along with newly emerging network technologies, while avoiding dependence on costly skilled technical support staff.

Except for the very smallest networks (less than 7 lines), a WAN implementation that uses remotely located distributed intelligence and operates on low cost Intel based servers, PCs, and routers, is certain to minimize both purchase costs and annual operating costs. The MMS can be used as either a single purpose AFTN-only WAN, or the base for a new organization-wide WAN that includes AFTN along with any other application. The MMS can also be implemented on any existing WAN. The MMS is far more than a simple **gateway** between an obsolete point-to-point network and an external WAN. Since the MMS AFTN system operates entirely on the WAN, it provides **all** of the advantages, such as high-speed transfers, maximum resiliency, and automatic error correction that cannot possibly be provided by a simple gateway to some external WAN.

Even if the MMS is initially installed as a simple point-to-point network, it can be upgraded at any time to the more advanced WAN technologies at a relatively low cost and impact, by simply adding WAN network routers. Since both the MMS software and the routers are multi-protocol, any combination of WAN technologies can be readily mixed on the same MMS system.

## 2 ICAO Compliance

The **MMS** is fully compliant with all items in the latest version of ICAO Annex 10. Additionally, in applicable areas such as flight plan validity checking and AMHS, the MMS is also compliant with :

- a) Procedures for Air Navigation Services – DOC 4444 – RAC/501
- b) Manual on the Planning and Engineering of the AFTN – ICAO DOC 8259 – AN/936
- c) Technical Provisions for the Aeronautical Telecommunication Network (ATN) Doc 9705

## 3 Operating System Compatibility

All components of the system operate under any version of the Microsoft Windows operating system from Windows 95 through Windows 2000, and Windows XP. The reason for choosing MS Windows over Unix or Linux alternatives is the result of the great importance that DRI places on the attribute of **vendor independence**. DRI believes this is also the reason that Windows has dominated all versions

of Unix (including Linux) in recent years in the number of new installations. Unlike software, hardware is subject to wear and failures caused by age alone. Therefore, it is much more important to be independent from hardware vendors rather than from software vendors.

All of the **supported** versions of Unix are proprietary to a specific hardware platform vendor. In the case of highly specialized applications, this means that any Unix based application must be 'ported' by its developer to run on more than one vendor's proprietary hardware platform. Because of the elimination of once dominant hardware vendors, such as Wang, Digital Equipment Corporation (DEC), Tandem, etc., software vendors are naturally reluctant to risk the expense of porting their Unix application to some other hardware platform. History has demonstrated that any Unix based proprietary hardware platform might very well disappear from the market in the near future. In contrast, there are literally hundreds of hardware vendors that offer MS Windows based systems.

Since the hardware platform vendors profit from the reduced competition that their hardware specific version of Unix provides, they are therefore able to sustain relatively high prices. These high prices are inevitable for the case where customers using specialized applications are permanently locked into the only vendor capable of maintaining or enhancing the application. Even worse, in cases where market forces eliminate the hardware vendor entirely (Wang, DEC, Tandem, etc.), the customers are left stranded with orphaned systems that are impossible to expand and eventually become impossible to even maintain.

For the above reasons, it should be apparent that the term "COTS" (commercial off-the-shelf) is often misleading. It is misused to provide reassurance to the buyer that is only an illusion. In many cases, it obscures the fact the product offered is highly proprietary and available only from a single vendor. The fact that 'Unix' is supposedly an 'industry standard' in no way mitigates the substantial risk that it locks the system buyer into a very expensive hardware system supplied and supported by only a single vendor. On any networked applications, where data can be readily interchanged between MS Windows platforms and Unix platforms via TCP/IP, there is no long term reason to become locked into Unix based proprietary hardware platforms.

#### **4 Hardware Composition and Testing**

Only 3 hardware components are used in the MMS: industry standard Intel-based servers and personal computers (PCs), wide area network (WAN) routers, and local area network (LAN) hubs. The server/PCs are used for message switching and routing at both the switching center and the remotely located front-end-processors (FEPs). The PCs also serve as end-user terminals for message origination and reception. The LAN hubs are used at the switching center and remote concentrator sites to connect together the switching server/PCs and the control, message correction, archiving, and monitoring terminals. The routers are also used at the switching center and at the remote concentrator sites.

At the switching center, the servers and PCs that are connected together on the LAN are either **switching server PCs**, or **terminal PCs**. The switching server PCs have no video monitor or keyboard and are connected to the routers. These server PCs perform the actual message switching and **high level** routing functions, through their connected routers. The routers perform the **low-level** routing

across the WAN. The LAN based terminal PCs allow the user to monitor and control the network, and also to prepare new messages and correct rejected messages. Terminal PCs always include a keyboard, mouse, and video monitor.

All components are 'commercial-off-the shelf' (COTS) items, but more importantly, all components are **non-proprietary**. To insure long-term maintainability, competitive prices, and to avoid future conflicts with operating system upgrades, no vendor specific hardware or software components are used. This precludes the use of any add-in cards that require a specialized vendor-specific software driver. This still allows up to the 4 standard COM ports and 4 LPT ports on PCs, since they are directly supported by the operating system. It precludes any 'multi-port' COM port add-in cards or add-in router interface cards, that require add-in vendor-specific software drivers. These vendor-specific cards pose serious long-term support risks, due to future incompatibility problems between device drivers and operating system software and product cancellation issues.

At least 7 competing vendors offer each of the 3 components that comprise the MMS. The switching center is composed entirely of servers and PCs connected on a dual-homed LAN. The front-end-processors (FEPs) at the remote concentrator sites use PCs that employ neither a keyboard nor video monitor. Depending on the application, a FEP may not necessarily employ a hard disk unit. On very large installations, this stripped-down FEP configuration is intended to further reduce the PC cost and approach the reliability of the routers and hubs that contain no moving parts.

In addition to the standard vendor hardware test programs and third party diagnostics, DRI provides additional specialized test programs for the LAN based units, and specialized simultaneous 4 port loopback testing on the FEPs.

## **5 Wide Area Network (WAN) and AMHS**

Although the MMS can be implemented as a point-to-point AFTN switch, or any hybrid combination of WAN and point-to-point architecture, the major cost reduction and resilience benefits are obtained for those networks which are entirely WAN implementations. It is also important to note that the MMS WAN is separate from the ICAO proposed Aeronautical Telecommunications Network (**ATN**). The MMS WAN is, however, fully compatible with the ATN. The ICAO ATN defines links between states, but does not mandate the much more numerous links within the state. Thus, the MMS WAN operates on the national AFTN level, while linking to other states at either the AFTN, Cidin, or ATN level. In the case of ATN links to adjacent states, the connectivity is provided through the ICAO defined AMHS gateway unit. The discussion below begins with the MMS WAN at the national level and near the end of this section it deals with the AMHS gateway link to the ATN.

The wide area network (**WAN**) consists of T1 or E1 lines, operating between 9.6 KBPS to 2 MBPS. Any combination of X.25, TCP/IP, Frame Relay, DSL, ISDN, or VPN network protocols can be used for the MMS. Additionally, V.90 or V.92 analog modems can be used, as either back-up or primary route, for any or all remote user lines. On the initial installation, depending on the network configuration, any of 5 possible Cisco routers are used. However, any other vendor or router model can be used to expand the WAN. All of these routers are multi-protocol, and 2 of the 5 routers are modular and

therefore easily expanded. The Simple Network Management Protocol (**SNMP**) is available, but not required, to monitor an X.25, TCP/IP, or Frame Relay implementation.

### ***5.1 Partial-mesh Considerations***

The number of telecommunication lines required for the WAN is based on the number of remote concentrator sites connected to the main switch. In order to take full advantage of resiliency designed into the MMS software, each concentrator site requires 2 lines. Since the 2 lines are typically connected to adjacent concentrator sites, they will normally be much shorter, and probably lower cost, than the alternative configuration of lines connected directly to the switching site in a star topology.

For example, a system consisting of a main switch and 3 remote concentrator sites requires only 3 lines if resiliency is not a requirement or if automated V.90 dial back-up is also implemented to provide resiliency. Assuming dial-backup is not implemented, then, for the elimination of service interruptions due to line problems, a total of 4 lines are required in order to provide the resilience of at least 2 paths to all sites. No matter how many concentrator sites are added, the cost-saving benefit of the resiliency provided by the single added line is more than justified. Adding yet another additional line increases the resilience and available bandwidth even further, although it is not essential. This method of adding lines, to provide 2 or more routes to any network point, is termed a 'partial-mesh' network.

The future ATN is an example of a partial-mesh network, at least at the inter-state level. Unfortunately, this ATN uses the costly to implement OSI protocols, making it impractical to extend to local AFTN users. Furthermore, the future ATN does not specify any partial-mesh requirements for the much more numerous intra-state links. Thus, at the local CAA level, the ATN permits the obsolete point-to-point links, which remain vulnerable to service interruptions. The overwhelming majority of AFTN system vendors can only offer a centralized switch with a gateway connection to adjacent states and point-to-point connections at the local level. Even though this limited gateway architecture satisfies the ATN requirements, it fails to offer the same resilience benefits that the future ATN offers on the inter-state links at the local level.

The primary reason why almost all AFTN system vendors cannot offer partial-mesh solutions at the local CAA level is due to the fact that the AFTN system software must be completely recreated to optimize the benefits of a partial-mesh WAN architecture. It is not possible to simply retrofit the old point-to-point AFTN software package to properly function in a totally new architecture. The software must necessarily be designed at the outset to interface with routers as part of a distributed network architecture. A secondary reason is that most AFTN system vendors have absolutely no experience in network design. The obsolete point-to-point installations never required any understanding of actual networks as such, and viewed the connections as nothing more than simple wires. As long as these vendors believe there is a reasonable chance of selling their obsolete point-to-point software, they will continue to avoid the very expensive and time-consuming development effort required to adapt to a partial-mesh WAN. Simply implementing an AMHS gateway to the ATN

allows these vendors to create an illusion that their obsolete point-to-point software is actually a modern up-to-date network solution.

### **5.2 SVC, PVC and Bandwidth Considerations**

The AFTN, F.31 or WMO application on the WAN use only a small fraction of the available router bandwidth and port connections. In the case of an X.25 application, this is achieved by delivering AFTN messages via switched virtual circuits (SVCs) 'calls', rather than permanently allocating bandwidth and ports, such as is the case in permanent virtual circuits (PVCs) or static SVCs. Once the queued traffic for that path is delivered, the 'call' is disconnected and the port becomes available for new incoming calls and the bandwidth becomes available to other non-AFTN applications. Thus at the time of initial installation, at least 80% of the ports and bandwidth of the routers are available for future applications, such as radar data, graphic weather maps, etc. These same SVCs are also critically important in providing resiliency outside of the WAN, since any remote station can be reached from the switching center via multiple servers, each connected to multiple routers.

### **5.3 AMHS and ATN Considerations**

An AFTN system based on a WAN for national users can readily coexist with the eventual implementation of the Aeronautical Telecommunications Network (ATN). The ICAO ATN provides connectivity between states and provides for a gateway unit, designated as an **AMHS gateway**, to link the national AFTN WAN to the inter-state ATN. Both networks can function on the same national WAN, regardless of any difference in protocols.

The AFTN/AMHS gateway provides for the conversion of the rarely used OSI protocols, mandated by ICAO, to and from the much more widespread industry standard protocols, such as TCP/IP, Frame Relay, VPN, etc. Thus, this gateway approach allows the national AFTN network to continually evolve as newer functions and services become available via the widespread industry standard protocols. The seldom used static OSI protocols can be isolated to only those relatively few lines between states, without imposing constraints on future enhancements to the national AFTN system. For reasons cited below, the optimum CAA strategy is to implement a TCP/IP and X.25 wide-area-network to replace any existing point-to-point AFTN system.

**Recommended Strategy:** There are numerous reasons to simply install a replacement AFTN system based on a standard TCP/IP and X.25 network, and then defer all aspects of the implementation of ATN and AMHS until the final version of the specifications have been issued **and** actual extended operational trials have been successfully completed. Up until now, only very limited and simplified point-to-point trials have been completed. The major high risk factors in ATN and AMHS involve the dynamic routing of large numbers of unproven OSI based routers interconnected in a partial-mesh between regions (inter-domain) and within regions (intra-domain). Even in the best-case optimistic schedule for the first regional large scale ATN pilot operational testing, it will be **2006** before this critical high-risk period will even begin. Unlike the ICAO mandated OSI protocols in the ATN router, the universal industry standard TCP/IP protocol based commercial routers have had the benefit of 20 years of operational testing in tens of thousands of units in private WANs, and millions of units in the public Internet.

Thousands of significant bugs and specification interoperability issues have been corrected during this 20 year period of live TCP/IP operation. Thus, *if* ICAO actually persists in using the OSI protocols in the ATN, then it will be **at least** 15 years before comparable stable operation is achieved in the ATN. However, at each new ATN Transition Task Force meeting, it is becoming more obvious that the OSI protocols must ultimately be abandoned in favor of the TCP/IP protocols. The three factors driving this major protocol revision are: **safety**, **economics**, and **deployment time**. All three of these factors apply to both the ground-ground router and the air-ground router.

The **safety issue** results from attempting to introduce a new highly specialized niche-market product (ATN router) across international organizations with no prior background or defined trouble-shooting procedures or OSI routing protocol experience. In fact, in the case of AFTN, all routing was manual, static, and strictly pre-defined and limited, and thus the introduction of automatic dynamic routing will be a first-time experience for all involved CAA support staff members. There will be no proven products or tested procedures, such as the case with TCP/IP based routers, to fall back on when routing problems and undetected software bugs cause a collapse of the international ATN.

The **economics issue** arises from the fact that there are only 2 vendors now offering ATN routers to a very small niche market, at a cost 15 to 30 times as great as comparable commercial TCP/IP based routers. The original ICAO expectations, of mandating universal ATN use to distribute and offset the ATN router development cost across all applications, has already been eroded by the acceptance of interim and regional adaptations such as 'AFTN over X.25' and 'AMHS over X.25'. It was even further eroded in April 2002 by the partial introduction of TCP/IP into the ATN world. This new position accepts AMHS over a TCP/IP-only based network that is not at all compliant with the ATN specification. It also accepts 'tunneling' ATN traffic over IP routers, thereby substantially reducing the market for the specialized costly ATN router.

The new ICAO position also recognizes that airborne IP networks already exist, and will now be considered for air-ground applications. Commercial TCP/IP services are now available that allow up to 9 airborne passengers to simultaneously access the public Internet using a normal LAN, or even a wireless on-board LAN. In the face of these alternatives, and with fewer than 200 CAA potential customers, it is extremely unlikely that this ATN router is an economically viable long term product. This uncertain ATN router outlook raises the serious issue of long term vendor support questions.

The **deployment time issue** results from the fact that significant routing and interoperability problems and latent software bugs won't even become visible until after 2006. Even if it were possible to realistically simulate the hundreds of ATN routers from all of the different regions in a single room, it would require 5 years of shakedown testing to debug the software and routing configurations enough to establish even a minimal confidence level. In reality however, this shakedown testing must take place across many widely separated support organizations, including independent service providers, speaking many different languages. During this crucial period the support staff is undergoing its first crash course in troubleshooting wide-area-networks. Even if there are no language problems, the challenge of regional or world-wide cooperative troubleshooting on an unproven new product will present a significant challenge. Much of this extended shakedown period could be eliminated by

simply starting out with the field proven commercial TCP/IP routers, with over 20 years of product development debugging periods behind them.

#### ***5.4 Protocol Translation***

Within the national AFTN system, the industry standard commercial router software handles any required protocol translation between any non-OSI protocols, such as Frame Relay and TCP/IP and X.25, etc., while the MMS itself handles any addressing conversion required locally, such as Telnet or X.121 to and from the familiar 8 character ICAO addresses. The MMS remote user terminals can be either the X.400 AMHS units or the standard MMS intelligent terminals. Since the standard MMS terminals use the familiar ICAO message format and provide even more capabilities and resilience than the AMHS defined terminals, there is no benefit obtained in undertaking the steep learning curve required by the AMHS terminals.

#### ***5.5 Mobile User and Wireless Considerations***

An example of the benefits of this strategy, of limiting the use of OSI protocols in favor of industry-standard protocols, is the MMS capability of connecting mobile AFTN users, and remote stations that cannot be directly cabled. In this case, PCs, notebooks, or hand-held PDAs can use wireless links to connect to the MMS WAN wireless access points at either the switching center or any remote concentrator. This link is handled via a combination of the wireless LAN protocols IEEE 802.11x and TCP/IP. For all wireless links security is provided by activating the built-in 128 bit industry-standard wired-equivalent-privacy (WEP) protocol.

The IEEE 802.11b protocol also provides a means to connect, to any remote concentrator or the switching center itself, any building complexes within a radius of 6 miles. This wireless connection is implemented by using very small directional antennas. Unlike the mobile wireless links above, this high-speed wireless link is between 2 fixed points. The one-time antenna installation and equipment cost is only a fraction of the annual cost of a leased line between the same two points.

#### ***5.6 VSAT Considerations***

The MMS can provide for VSAT links between the switching center and the remote concentrators and/or between remote user stations and the switching center. As a result of the multi-protocol capability of the MMS software and routers, the MMS can even be used as a gateway or bridge between 2 different VSAT networks employing different protocols and satellite access methods. The combination of VSAT, with automated dial back-up, provides the absolute lowest cost method of providing highly resilient connectivity by minimizing or eliminating the much more costly leased land-lines.

The MMS also offers the possibility of eliminating any VSAT Frame Relay monthly service charge. Since the AFTN switch itself functions as a hub, the links can be implemented in a star topology as either TCP/IP PPP, Telnet, X.25 PVC or SVC, or simply V24. Wherever it is available, implementing the VSAT links in a star topology also makes it possible to avoid the more costly TDMA satellite access method in favor of the minimal cost MCPC/FDMA or SCPC/DAMA method. For those cases where a

regional VSAT network is involved, the MMS makes it possible to use Frame Relay only on the regional VSAT link, while employing TCP/IP PPP on local AFTN non-regional VSAT links.

## **6 AFTN WAN as General Purpose CAA Network**

Ultimately, all CAAs will implement organization-wide administrative WANs for data interchange. Equally certain is that all AFTN systems will be eventually implemented on a WAN. For obvious cost reasons, these 2 applications should share the same physical network. Once the AFTN network is implemented on a partial-mesh WAN, the infrastructure is already in place to extend its functionality to a general purpose administrative network for the entire CAA organization. The same routers and links used for AFTN can readily be adapted to TCP/IP based servers, LAN switches, and personal computers throughout the entire organization. Since TCP/IP is essentially the universal protocol, any Windows or non-Windows server, work station, or personal computer can be accommodated by the infrastructure.

Thus, the AFTN network becomes part of an organization wide intranet, that provides e-mail, document collaboration, file transfer, etc., services between staff members in different locations. As an intranet, it also can be used to provide local web-site hosting that all staff members can access with commercial browser programs, such as MS Internet Explorer or Netscape. Wherever it is necessary, the AFTN network can be kept functionally separate from the general purpose network by the installation of virtual-private-network (VPN) units that incorporate built-in firewalls. For those cases where the CAA has an existing WAN in operation, then the MMS AFTN system can be installed as a component of the existing WAN, with VPN/firewall units isolating the AFTN system from other non-AFTN network users.

## **7 Software License**

The MMS can be expanded at any point in the future by simply adding industry standard servers and PCs and implementing the DRI software packages for the MMS component added. In addition to the servers and PCs at the switching center and FEPs, this also includes adding dial-up and/or directly connected message preparation and editing terminals running the DRI MMSTERM software package. Providing the use of the MMSTERM program license to the end-users makes it possible to implement an error-correcting Ack/Nak protocol, with WAN connectivity and/or automated dial-up access. This user terminal license applies throughout the entire network at no additional costs, regardless of how many users are added in the future.

## **8 Capacity**

Each of the server PCs comprising the switching center can handle 150,000 messages per day without introducing any significant message delay. Each single switching center can be expanded to 30 switching servers and PCs, for a maximum capacity of 4,500,000 messages per day. A typical switching center of 7 servers/PCs, routers, and hubs can be installed in a single rack. The expanded system of 30 server/PCs, and the associated hubs and routers, can be easily installed in 4 standard equipment racks. If the traffic load exceeds 4,500,000 messages per day, then additional switching

centers can be implemented and linked to the initial switching center by either WAN links or LAN switches.

## 9 Reliability

The switching center and remote concentrators automatically distribute the traffic load across all the server PCs. For reliability, at least 4 server PCs must be installed. Although an ordinary PC can readily function as a switching PC, the MMS normally uses Intel based servers from IBM, Compaq, Dell, Hewlett-Packard, etc., as the switching units. These servers include RAID level hot-swappable hard disks and error-checking-and-correction (ECC) RAM. If a server PC fails, the remaining PCs automatically pick up the load of the failed server PC without any operator intervention. If somehow 3 out of 4 server PCs failed simultaneously, the remaining single server PC automatically carries the entire traffic load. However, even a single remaining server PC is capable of handling at least 200,000 messages per day by gradually accumulating message queues (backlog). Although a single server PC handling message loads above 150,000 messages per day might eventually introduce message delays, the system continues to function in a somewhat degraded fashion. Normally, at least one of the 3 failed server PCs would be rebooted and returned to service long before any queue at all developed.

Thus, as long as at least one of the server PCs is still operating, the system will not crash. By connecting each of the PCs and both LAN hubs to separate small dedicated UPS units, each fed from separate AC power sources, a system crash is virtually impossible. This yields a system availability of 99.999 % ('**five nines**'). If somehow both LAN hubs failed simultaneously, the message traffic continues without interruption or delay, since each of the switch server PCs are autonomous and independent of any other PC. Each server PC is connected to at least 2 routers through serial ports in addition to its LAN connection.

Each node in the system is capable of holding up to 2,000 messages on its individual queue. For example, if there were 6 switching center server PCs and 12 FEPs handling 6 remote concentrators, then the combined distributed queues, between the switch PCs and the FEP PCs, can indefinitely hold at least 36,000 messages in the event of a prolonged major nationwide communication line outage. If an operator is present to put some of the blocked destination traffic on hold, then over a million messages could be retained indefinitely until the communication lines were restored. If automated dial-backup to the concentrators is implemented, then not even a total failure of the network itself can cause a service outage.

Although LAN hubs and routers crash only about once in 12 years, servers and PCs crash more frequently. This higher rate of PC failure is the result of intermittent faults due to moving parts and operating system flaws. However, in almost all cases, the server or PC can be quickly restored to service by simply rebooting it. Thus, a server PC needs to be replaced only for a hard recurring fault, which typically occurs about once every 7 years for a brand-name server employing hot-swappable RAID drives and ECC RAM. For an ordinary PC, a recurring hard fault may occur as often as once every 3 years. Therefore, in the typical case of 6 switching units sharing the traffic load, the

approximate mean-time-between-failure (MTBF) is 46,000 *years*. If ordinary PCs are used as the 6 switching elements, this MTBF drops to 216 *years*.

Thus, in either MTBF case, a total system failure is virtually impossible, barring a catastrophe such as a flood, fire, or explosion. Even in the event of a physical catastrophe, it is still possible to maintain service without interruption if the option for a remotely located contingency switch is implemented. This option is described in a later section of this document.

## 10 Resilience

Within the MMS network, there is no 'single-point-of-failure', such as is common on the obsolete dual-mode hot-standby architectures. This MMS redundancy applies not only to the communication paths between the routers, but also between FEPs and their associated end-user terminals or printers. All possible message flow paths for each route are continually used in a load-balanced manner. This is done in order to avoid the problem of an idle fall-back line that is out of service for weeks without detection, until it is actually needed. If any of the paths are blocked or develop high message queues, the system automatically shifts all the traffic to the remaining good paths without any need for operator intervention.

If all paths to a particular user station or FEP are blocked, then the system recirculates the traffic within the system, until at least one path is restored, or the operator establishes an alternate route. When the faulty path is restored to normal service, the system then automatically resumes distributing the traffic across both paths. Thus, at a level **above** the WAN, the MMS system automatically 'routes around' problems *outside* of the WAN, in the same manner as the routers themselves do for faults *within* the WAN.

The fact that the MMS typically operates on a **digital-based** WAN, provides added protection against corrupted messages that are typical in the standard noise-prone **analog line** point-to-point AFTN system. Since the routers and all PCs and dial-up modems in the system employ error-checking and correction in addition to digital lines, communication line problems are virtually eliminated.

## 11 Long Term Cost of Ownership

Since the MMS is composed of relatively low cost components, its initial purchase cost is typically much lower than the comparable obsolete point-to-point AFTN system. Within 2 years however, the ongoing long term cost of ownership (LTCO) savings of the MMS, over the point-to-point system, is much greater than the initial purchase cost savings. This is the result of the following factors:

- Line costs are reduced, with 4 to 7 **digital** WAN lines replacing 30 - 500 lower speed **analog** communication lines.
- Line costs are reduced for any station transferring less than 250 messages per day by implementing automated on-demand V.90 dial-up calls.
- Line costs are reduced by converting, on an ongoing basis, all or some lines to newer emerging low cost network technologies, such as Frame Relay, VSAT, ISDN, DSL, VPN, or V.90 dial-up.

- Elimination of 24/7 hardware maintenance staffing costs by added resiliency, and the total elimination of local component level repairs. All hardware maintenance is reduced to highest level unit replacement only. (See section 13 below).
- Reduction in operator staffing costs due to the elimination of communication line problems, which otherwise would require message correction or reentry by operators.
- Reduction in operator staffing costs due to automated alternate routing on hardware problems, and fully automated service-message handling and retrievals.
- Reduction in cost of on-site spare parts resulting from very low cost components from multiple competitive sources, and duplication of on-line units.
- Reduction in line costs and staffing by distributing costs over a combined AFTN and administration wide IT network that shares the same network infrastructure. (See section 6 above).

In addition to reduced LTCO, the MMS may make it possible to reassign scarce technical staff to other functions which might be critically under-staffed.

This lower LTCO is likely to become increasingly important, as indicated in recent ICAO Journal articles. Those articles described the growing pressure from airline companies on ATC service providers to reduce user charges, regardless of whether they were semi-state, fully privatized or otherwise. The argument to reduce charges was supported by cost comparisons of various services between comparable ATC service providers. Thus, even if the current AFTN system has not reached the end of its life-cycle and is still supported by the original vendor, it may still be economically necessary to replace the system in order to reduce ongoing operating costs.

In the case where an obsolete point-to-point AFTN system is replaced by a 'partial-mesh' WAN, the saving in operating costs can typically repay the entire cost of the new AFTN system in less than 2 years. Assuming that a typical system connects 40 user stations on 40 directly connected lines, and each line costs approximately \$ 8,000 per year, then the leased line costs are approximately \$ 320,000 per year. If the 40 remote user stations can be concentrated into 4 remote sites, then the leased line costs drop to \$ 40,000 per year for the remaining 5 lines required for the new MMS. Thus, the annual operating costs are reduced by \$ 280,000 each year, and in 2 years the new system saves \$ 560,000 in line costs alone. Depending on traffic loading, it may be possible to use automated dial-up calls to even eliminate some of the 5 remaining lines for further annual savings.

## **12 Connectivity and Scalability**

The MMS can be expanded very economically almost without limit, simply because it is implemented on a WAN. This expansion can be achieved by adding modules to the routers, and/or activating currently uncommitted router ports. Unlike a point-to-point AFTN system, where adding a user terminal means adding a new costly communication line, the WAN simply utilizes more of the available bandwidth on the existing switch-to-concentrator communication line. The discussion

below assumes a worst-case requirement, where the primary AFTN link must be via X.25 SVC connections. For TCP/IP implementations, expansion is much simpler and requires far less hardware.

At the switching center, the initial 4 or more switching server PCs can be easily expanded up to the practical limit of 30 switching servers or ordinary PCs. Since the dual LAN is a relatively simple peer-to-peer LAN, it is an easy matter to add PCs without modifying any complex file server. Since each server PC connects to 2 different routers, this means that a total of 60 router ports are required to accommodate this maximum expansion for X.25 SVC connections. Both types of Cisco routers normally used in the MMS are modular routers, capable of expansion by adding circuit cards. Thus, added ports can be obtained by adding modules to the initially installed routers. If this provides less than the maximum of 60 router ports, then the remaining router ports can be obtained by simply concatenating new routers to the existing routers.

The total of 60 SVC router ports at the switching center would be approximately matched by 120 SVC router ports at the concentrator sites. This 'concentration ratio' of 2 to 1 is very conservative, and a ratio of 5 to 1 has been tested with only moderate message delays introduced by call set-up delays. Each router port pair at the concentrator site allows connection to 30 added user terminals, while still providing the full resilience of 2 independent message paths for each terminal.

Thus, the 120 SVC router ports at the concentrator sites provides for the connection of 1,800 user terminals. Since each switching server PC can handle 150,000 messages per day, the total daily throughput of the switching site (4,500,000 messages per day) allows for an average of 2,500 messages per day per user terminal. Only a very small fraction of AFTN user terminals generates this level of daily traffic. Since each of the 1,800 user terminals can also connect its own free COM and LPT port(s) to additional single-path terminals, at least 3,600 total terminals can be accommodated without implementing a second switching site.

### **13 Maintainability**

The switching center Reports position monitors the status of all external FEPs and ports. Each FEP must report its own status, and all connected user station status conditions, to the switching center every 5 minutes. On the switching center dual LAN, a LAN control PC monitors the status of all servers and PCs comprising the switching center itself. Each LAN based PC must report its status to the LAN control PC every 3 minutes. Thus, if any PC fails, it is reported by name on either the LAN control unit or the Reports unit. In both cases, an incoming status report is considered overdue one minute after the end of the reporting period and is therefore reported to the Reports position.

If one of the 2 LAN hubs fails, it will be automatically reported on the LAN control PC and readily identifiable visually by the absence of blinking on the activity indicator light, or the absence of all port indicator lights if the power fails. In either case, the system continues running on the remaining good LAN hub.

If a router fails, it will be identifiable by error reports from the FEPs or the switching PCs directly connected to that router. If SNMP is employed, then the WAN network monitor display will also identify the failed router.

In all 3 above cases, the problem is much more likely to be intermittent, rather than a hard failure. Therefore, the initial corrective action is typically to reboot, or power down and then power up the failed unit. If this step does not clear the problem, or maintenance records indicate frequent errors on the unit, then the unit must be replaced by the on-site spare whenever maintenance staff is available.

Since the PCs have either 4 COM port connections, in the case of FEPs; or 2 LAN and 2 COM port connections, in the case of switching center server PCs; it requires only 15 minutes to replace a server or PC with its on-site spare. Even if the server PC is not replaced for days, it will have little or no impact on the traffic, since the remaining alternate paths automatically redistribute the message traffic.

If a router fails and cannot be rebooted, then the on-site spare must be used to replace the failed router. This task may take up to 25 minutes, since there may be more cables involved and the specific routing tables must be installed in the replacement router if protocols other than TCP/IP are used. The installation of the routing tables is simplified by a DRI supplied utility program, that reads the router tables from a floppy diskette and automatically loads them into the replacement router. No keyboard, display or manual intervention is required. It is only necessary to connect the FEP COM port to the router console port, and then power up the FEP from the specific diskette containing a copy of the router tables. Alternatively, the router tables can be downloaded from any of the server PCs or operational PCs directly to the router LAN port.

To summarize, assuming a reboot doesn't clear the problem, hardware maintenance is now reduced to the following actions, none of which requires even a screwdriver:

- (a) Disconnect 4 to 8 clearly labeled cables and power down the unit.
- (b) Remove one box and replace it with an identical box.
- (c) Power up the unit and reconnect 4 to 8 clearly labeled cables

Considering the high degree of resiliency, the above 3 steps do not have to be performed on a demand basis. Instead, they can be scheduled for a convenient time when staff is available.

Because of the very low cost of LAN hubs and PCs, especially without video monitors, it is not necessarily economically prudent to spend any time attempting to repair the failed unit. If it is under warranty, it can be returned to DRI or the vendor. Alternatively, it can be sent to the local computer store for a service contract repair. In the case of the much more expensive router, after the initial warranty period, it may be worthwhile purchasing an annual service contract from the router vendor, rather than paying for repairs on a per-case basis. Typically, the annual service contract results in quicker turn-around, and Cisco provides good international 24 hour technical support at a very low cost.

## **14 Communication Interfaces**

The MMS supports V24/V28 (RS-232), RS-422, RS-423, current loop, and all of the various synchronous and asynchronous digital interfaces provided by the Cisco routers. The Cisco routers

handle baud rates from 300 BPS to 2 MBPS. The switching PCs and FEPs handle baud rates from 50 baud to 115 KBPS. The number of data bits per character varies from 5 bits for Baudot code to 8 bits for ASCII code.

The MMS supports both ITA2 baudot and IA5 ASCII codes as defined in ICAO Annex 10. It also supports a hybrid combination where the ITA2 SOM (ZCZC) and EOM (NNNN) are used with the IA5 code set. In IA5 both upper and lower case is accommodated, in both the message text and the message envelope. The upper/lower case attribute is passed transparently, or converted to upper case based on a user settable parameter.

The MMS also supports X.28, Telnet, PPP, SLIP, V.90, and Cisco PAD interfaces on any of its COM ports, in addition to TCP/IP, Frame Relay, DSL, cable modem, VPN, and X.25 on LAN ports. In the case of VSAT connections the MMS can provide either Frame Relay or TCP/IP PPP interfaces. Since the MMS switching center can also act as the VSAT hub, it is possible to reduce operating costs by avoiding the Frame Relay service charges on the VSAT links. In addition to VSAT other wireless LAN connections are available through IEEE 802.11a, 802.11b, and 802.11g. These WLAN allow mobile AFTN users to send and receive messages anywhere within 100 meters of a wireless access point connected to either a concentrator site or the switching center itself.

## **15 Error Checking and Control**

In the case of both X.25 and TCP/IP, error-checking and correction is inherent in the router-to-router WAN protocol. Beyond the WAN routers, the switch and FEPs and the connected user terminals also employ an error checking and correcting ACK / NAK protocol at a level above the highest router level. In the case of SVC calls, this ACK / NAK protocol provides for up to 45 attempts before encapsulating the message and delivering it to the system Reject position. To preclude tying up the router port, the 45 attempts are grouped in 3 sets of 15 attempts each, with 3 minutes delay between sets. On each new call attempt, a different port and selection number is used than the one that just previously failed. Thus, in the case of an SVC call inbound to the switch, the 45 call attempts for that message will automatically be distributed across at least 10 different router ports and linked PC ports.

In addition to the above hardware error correction, the ICAO-mandated format checking is performed at every step in the transmission of the message between the switch server PC and the end-user terminal. This includes the checking of message sequence numbers and validity testing the elements making up the AFTN 'envelope'. Any format error detected at any point causes the message to be diverted to the system Reject position with a 'plain language' description of the format error. Alternatively, a configuration parameter can be set to automatically return the message containing the format error back to the originating station. This method reduces the work load at the switching center by placing the obligation to correct the format error on the source of the message.

The ICAO Annex 10 defined Check message is also handled by the MMS. In addition to the standard 20 minute interval between Check messages, the MMS can be set, on a per circuit basis, for any interval as little as 1 minute between Check messages.

## **16 End-to-End Loopback Checks and Confirmation Messages**

Any terminal or FEP in the network can send a 'loopback command' to any other PC in the network. The PC receiving this loopback command generates a detailed status report and sends it back to the requesting terminal. The status report includes current and cumulative message counts, error counts, cumulative out-of-service minutes, last sent and last received message sequence numbers, etc. Using this tool, it is possible to check on the status of any (or all) of the major elements in the network from any single terminal anywhere in the network. Both the initial command and the resulting response are encapsulated as actual AFTN messages, so they check the complete normal routing path through the switching center server PCs and the routers themselves.

In addition to the loopback check, any user can invoke, on a per-message basis, a function that demands a confirmation message back from the intended destination terminal confirming the receipt of the message. The sender can specify that the confirmation message is to be sent on receipt of the message or only when the message has been viewed or printed. A configuration parameter can be set to determine how long the sending terminal will wait for confirmation before resending the message. Another configuration parameter can be set to specify how many times the message will be repeated before the sender is notified of the non-delivery. As long as the MMS terminal is in service, it will automatically respond to any incoming message that requires a confirmation back to the sender.

## **17 Automatic Repeat Request and Response**

The ICAO Annex 10 requirement for SVC QTA MIS and SVC QTA RPT service-messages is entirely automated in the MMS. An information message is automatically sent to the system operator control position to inform the operator of the action automatically carried out by the FEP. A user-settable parameter, on a per circuit basis, sets the maximum number of messages that are automatically retrieved and resent in response to a single request. Conversely, a user settable-parameter limits the maximum number of missed messages that the FEP will automatically request from the adjacent unit.

## **18 User Interface**

The user interface consists of pull-down menus and pop-up dialog boxes used to carry out operator commands. There is never a case where the operator has to type more than 10 characters to carry out the command. Some of the more complex and infrequently used operations, such as specialized message retrieval functions, automatically pop up a help message box containing detailed information about the command. In the case of status or any other information request, the requested information is displayed on the screen immediately. An Alt-H keystroke combination brings up a scrollable and searchable pop-up Help screen that lists all commands available to the operator, with a brief description of the command.

An online pull-down Help sub-menu can be customized by the user to describe system specific operational procedures, such as alternate routing instructions, contact numbers for adjacent AFTN sites, listing of collectives, listing of abbreviated addresses, current staff schedules, temporary changes to normal operational procedures, display of current routing tables, etc. Any of the displayed Help files can be searched for any key word(s) required.

## **19 Predetermined Address Lists (Collectives and broadcast messages)**

In addition to satisfying the requirements of ICAO Annex 10, the MMS makes possible the definition of large distribution lists from a single ICAO address. For example, multiple distribution lists can be created by the user, each invoked by a single unique ICAO address, each one capable of regenerating the message to address as many as 400 ICAO addresses. This collective/broadcast list function can be useful in distributing weather information and NOTAMS, and any other type of message that must be sent to a large group.

This predetermined address list functions at the switching center acting on any received incoming message. This function is separate from the **abbreviated address** function, which operates locally at the user terminal and is described later. An abbreviated address at the user terminal can expand locally into one or more addresses. These addresses may also include 'collectives', which are then even further expanded upon reception at the switching center.

## **20 Configuration Control**

All of the operating parameters, including individual circuit parameters, are established by user created text files. Thus, any simple text editor, such as Notepad or Edit, is all that is needed to change any configuration, including the routing tables. All configuration data is checked for validity and any errors are reported when the server or PC is started.

In the case of routing table configuration, a special safeguard is applied to detect and remedy the routing problem whereby a message circulates indefinitely within the AFTN network ('circular routing'). In this case, after 40 routing actions have occurred on the same message, this message is then encapsulated and sent to the system Reject position with an appropriate error notice.

## **21 Functional Assignments and Automatic Reconfiguration**

Of the 7 or more PCs on the LAN that connect the switching center units together, 3 of the PCs are assigned functional roles, such as system archive, system reports, system alarms, LAN control, and message reject and correct. These assigned roles do not preclude the operator from originating a new message on any of the LAN connected PCs, even including the server PCs. These roles are assigned at start-up based on configuration files and are instantly displayable on all of the PCs. These functional roles can be distributed across all of the PCs, or assigned to a single PC. However, these roles can be reassigned at any time, by the operator, to any other PC on the LAN. Thus, if it is necessary to remove a PC for servicing or replacement, the operator can choose which of the other PCs will be assigned that role served by the unit being removed. In the absence of an operator choice the defined default backup is assigned.

The configuration files also determine whether or not certain functional roles will be automatically switched, in the event of failure of the PC currently serving that particular function. For example, if the configuration is set to preclude the system archive role from being switched, and that particular PC failed, then the system would temporarily be without a system archive unit. In this case, however, all of the other servers and PCs would now hold their own archive data until some PC was assigned

the system archive role. Once that assignment occurred, these servers and PCs would now unload all of the locally stored archive data into the newly assigned system archive PC.

## 22 Routing Control

Each server and PC at the switch and all Front-End-Processor (FEP) PCs have their own routing tables. In effect, each FEP is a small scale AFTN switch in itself. Message traffic leaving the switch, for a particular destination, is sent via router and WAN line to a specific FEP. Since there are always at least 2 paths for any route, the next message to the same destination will be sent through a different router and FEP serving that same route. If there are 3 or more FEPs serving that route, then the switch will treat the list of FEPs on a 'rotary' basis, to ensure that all active paths are continually used.

If the message sent to a particular FEP can not be delivered, due to a hold condition or high queue load on the next intermediate link, then the FEP automatically returns the message to the switching center. The switching center then automatically sends this same message to a different FEP on the same route. If that FEP is also blocked due to a hold condition on the next link, then this second FEP also returns the message to the switch. This recirculation of the message continues until either the intermediate link is restored to service, or the entire destination is put on hold, or an alternate destination is assigned by the operator.

## 23 Alternate Routing

In addition to the **automatic** alternate routing described above, the operator can override any automatic alternate route, by assigning a new route for a particular destination. In doing so, the operator will be redirecting this traffic to a different pair of FEPs than would normally receive it. This routing control operates at a level above the automatic routing provided by the WAN routers. This AFTN level alternate routing step can be performed quite easily by simply entering the 2 destination numbers involved, and then confirming the action with another keystroke. To protect against incorrect alternate routing assignments misdirecting traffic to an invalid route, this newly assigned pair of FEPs must have entries in their own routing tables that accept this particular alternate routed traffic. If there are no entries, then these FEPs immediately reject the message during the delivery attempt. This rejection forces the switch PC to encapsulate the message and divert it to the system rejects position, with an appropriate error message. This rejected message alerts the operator to reassign this traffic to a valid alternate destination.

A pop-up information screen(s) displays all of the destinations, along with the default direction, and the current alternate destination if activated. Each destination that is currently redirected is flagged with 2 asterisks to make them easily noticeable. If any destination is on hold, then the current message count accumulated in that particular hold queue is displayed along with the asterisks.

## 24 Load Balancing

Within any MMS switch PC, or any FEP, there are usually 2 or more different serial ports, in addition to the LAN ports, to choose from in onward routing of a particular message. In order to avoid any message delay resulting from high queue loads, it is desirable to perform load balancing by selecting between 2 or more possible ports. If one of the ports is on a hold condition for any reason, then the

remaining port(s) is unconditionally selected. However, if all ports are serviceable, then the routing algorithm selects the port with the fewest messages on queue. If there are no messages as in the normal case, or all choices have an equal number of messages on queue, then the algorithm selects the one with the least cumulative total output traffic for the day.

## **25 Message Retrieval Functions**

The most common method of message retrieval is by channel ID and output sequence number (CSNO). This type of retrieval is carried out automatically by the FEPs, in response to an incoming SVC QTA MIS or SVC QTA RPT service message. Each FEP circuit has a settable parameter that establishes the maximum number of messages that will be retrieved in a single request (typically 30). For each retrieval to the requesting terminal, the FEP also sends a detailed 'results report' back to the switch operator position.

Additionally, the operator at the switching center can cause any FEP to send retrieved messages to either the original recipient, or back to the user terminal on which the operator entered the request. This operator command requires typing only the 10 characters for the starting and ending CSNOs (for example: SLA345-444). In the case of retrieval commands from the switching center, the FEP will allow up to 100 messages per single command. Depending on the speed of the FEP CPU chip, 100 messages can typically be extracted and queued for delivery in approximately 15 seconds. The length of time required to retransmit the retrieved messages is a function of the baud rate for that circuit, or the WAN speed in the case where they are returned to the switching center. Depending on the level of traffic, the FEP typically holds all messages for at least 12 hours. Any retrieval of messages older than 12 hours may require the system archive in the switching center.

At the switching center a variation of the retrieval function provides for a full message trace based on message control field criteria. For example, by retrieving based on the embedded MMS message sequence number of the incoming message, all resulting output messages will be collected. Regardless of the selection criteria used to retrieve the messages, the entire collection is saved to a file which is paged up on the screen for viewing at the completion of the retrieval command. From this displayed collection of messages the user can easily select any message to be retransmitted to the original destination. It is also possible to automatically retransmit the entire collection by a single operator action.

All of the messages can be retrieved at the system archive of the switching center by other criteria rather than simply the CSNO range. This includes input circuit, origin indicator, destination, direction, or even the text content of any part of the message. This more sophisticated retrieval allows the operator to specify starting and ending times, and even starting and ending days where the search must span multiple days.

Another variation of this more sophisticated retrieval command is provided by commands to selectively narrow the number of messages retrieved. For example, by using this more selective command, it is possible to select only messages containing flight plans for KLM, arriving on the EuroControl input circuit, and addressed to a specific Flight Data Processing system, with a message origination time between 1535 and 2213 hours.

## **26 Message Archiving and Storage**

The PC serving as the system archive is normally equipped with a removable drive or cartridges of 250 MB or greater. This drive can be used to copy the hard drive daily archive file for an off-site backup. However, since all of the switch PCs contain disk drives of at least 10 gigabytes, this cartridge drive does not necessarily have to be used at all. Depending on the daily traffic load, the daily archive file will typically range from 40 MB to 200 MB. Thus, it is quite possible to satisfy the ICAO 30 day retention requirement by simply copying the daily archive file to any one of the other 7 PCs on the LAN. This provides 2 copies for all 30 days in 2 different PCs.

For systems handling extremely heavy traffic loads, it is possible to compress the daily archive before storing it on the removable cartridge. Since text-only data compresses at a ratio of approximately 10-to-1, the removable cartridge can accommodate 2.5 gigabytes of data. At least to date, the most heavily loaded AFTN system in operation anywhere generates less than 180 MB of data. Since the MMS uses addressable drives under the MS Windows operating system, any new techniques or devices such as network attached storage (SAN) can be automatically incorporated into the archive function.

## **27 Built-In Text Editor**

All MMS terminal units include a built-in text editor. The editor includes all the normal editing functions, such as 'file save' and 'file load', 'cut and paste', 'word-wrap', 'file insertion at cursor position', 'search', 'search and replace', 'undo', etc. User-settable parameters determine the appearance and behavior of the editor, such as block cursor, blink rate, color and font selection. This editor can be used to create any size AFTN message, by either typing or the insertion of prepared text files. Files can be easily concatenated on screen to create customized 'canned messages'.

## **28 Message Validation and Envelope Generation**

All messages entering the MMS system are subjected to an Annex 10 format validation check at the entry point to the system. If any errors are detected, the original message is encapsulated and a 'plain language' error message is appended and then sent to the system Reject position for correction. Optionally, this faulty message and appended error notice can instead be returned to the sending station for correction.

For any message typed on any MMS terminal unit, a full AFTN envelope is generated automatically. Usually, only the address must be entered by the operator. However, if the message is intended for a frequently addressed station(s), then it is possible to set a parameter so that a default list of addresses is automatically inserted. In fact, a single or multiple character 'abbreviated address' can be used, which is immediately expanded with up to the maximum of 21 addresses allowed.

Once a message has been prepared, and the AFTN envelope automatically generated, it is still possible to accidentally corrupt the message format by over-typing or typing a line that exceeds the ICAO allowed maximum line length. Therefore, when the message transmit function key is pressed, a final validation check is performed. If any errors are now detected, the cursor is placed on the incorrect element and an exact description of the error is popped up.

## **29 Address Book**

After any message has been prepared and the AFTN envelope has been generated, the operator can pop-up an ICAO address book to select the normal ICAO address or an abbreviated address, which expands to a list. The address book is created and updated with a simple text editor. Each entry contains the ICAO 8 character address and a description/name field of up to 50 characters. This description field can contain anything, such as an organization name, functional name, or the name of a person. For example, an address book entry might contain 'names' such as 'UK Weather Query 3', or NOTAM Distribution List 1' or 'Flight Plan submit' or 'AIS/OpMet Office', etc.

In an adjoining column to the name/description column, the actual 8 character ICAO address would be included. The cursor selection bar is placed on the desired entry, and the Enter key then inserts that ICAO address or address list at the proper point in the message envelope. If, instead of an 8 character address, an abbreviated address of 1 to 8 characters was listed, then that abbreviated address is then expanded up to a maximum of 21 ICAO addresses.

## **30 Oversize Message Handling**

Any size message can be created using the functions of the built-in text editor, including loading any text file from any accessible directory anywhere on the disk. Regardless of how large the message, the operator can automatically send it in segments that satisfy Attachment D of Annex 10 Volume II. By using a special key to transmit the message, the normal 'overlength' check is bypassed, and multiple messages are generated and queued for transmission by segmenting the single large message on the screen into however many smaller messages are required.

## **31 On-Line Statistics and Reports**

Every 5 minutes, each FEP sends in a detailed status report to the switching center. This status report covers all communication lines on that FEP. The data sent includes the message counts in and out, and both current and cumulative daily count. It also includes current line errors and cumulative daily line errors, in addition to the current and cumulative number of minutes out of service, number of service messages sent and received, the number of messages on queue, and the reason code for any hold condition.

A key combination is used to view the overall current status of all of the FEPs and switching PCs in the system. Another key combination is used to instantly view all of the circuit conditions described above, grouped by FEP, in a single scrollable, searchable on-screen report. A third key combination prompts for a circuit number and then displays a summary of all the 5 minute status reports from midnight up to the current time. At midnight there will be 288 single summary line entries making up the report. This report also breaks out hourly subtotals and makes it very easy to determine peak traffic periods either on an hourly basis or 5 minute interval.

All of these daily reports are retained in a history line status directory. After a certain number of days, the oldest reports are automatically erased to avoid eventually filling up the disk. Since these reports are delimited text lines, they can easily be imported into a spreadsheet for more detailed analysis.

## 32 System Monitoring and Control

The switching center Reports position monitors the status of all external FEPs and ports. Each FEP must report its status to the switching center every 5 minutes. On the switching center dual LAN, a LAN control PC monitors the status of the 8 servers and PCs comprising the switching center itself. Each LAN based PC must report its status to the LAN control PC every 3 minutes. Thus, if any PC fails, it is reported by name on either the LAN control unit or the Reports unit.

If one of the 2 LAN hubs fails, it will be automatically reported on the LAN control PC and readily identifiable visually by the absence of blinking on the activity indicator light, or the absence of all port indicator lights if the power fails. In either case, the system continues running on the remaining good LAN hub.

Whenever there are more than 100 messages on any specific circuit queue, then that queue is reported by the FEP to the system operator every 15 minutes, until the total number drops back below 100. Any time there is a change in the input and output circuit state (such as a required modem control signal) that change is reported immediately to the system operator. If the loss of a required modem control signal implies an interruption in the message path, then the output traffic for that circuit is automatically put on hold. If any circuit is on any kind of an output hold condition, this 'hold-state' is reported every 20 minutes until it is cleared.

In addition to circuit conditions imposing an immediate and automatic output hold condition on any circuit, the system operator can also send specific commands to the FEP to turn off a circuit entirely, ignore circuit input, or put circuit output traffic on hold.

## 33 System Clock

The switching center LAN control unit acts as a master clock for the entire network. Every 10 minutes this unit sends date and time commands to all the other units on the LAN. Then, every 20 minutes, the system Reports position sends date and time commands to all FEPs. Normally the FEPs are 8-12 seconds behind the LAN control unit due to the transmission time of the command.

The MMS system also provides for the use of an external reference clock, such as that derived from a GPS receiver. In this case, the time and date information must be supplied in a common defined ASCII text format.

## 34 Built-In and Definable Message Templates

**Message Templates:** A function key pops up a list of ATS and OpMet message templates. The default set of 40 templates can be customized and expanded by the user. Even the colors of the fill-in fields and captions, and the contents of the help notes, are customizable by the user. Multiple variations of the same type of template can be included in the list. For example, a user may require 3, 4, or 100 variations of the flight plan template to cover the most common cases of typical flights. In addition to the supplied set of 40 message templates a facility is provided so that the users can define their own templates for future use.

Within each template the fields are automatically filled in wherever possible, and editable default text can be included in any field. The ECT performs error checking on a field basis, as data is keyed in by the user. Error checking can also be performed at any time on the entire template by pressing the 'F2' key. A running count of the current error number and the total error count are presented in the error message box.

**Template Playback:** Even after a filled-in template has been converted to message form, it can be restored back to template form for further editing. This is done using the 'playback template' entry. This feature also allows the most recently transmitted message to be 'played back' in template form to serve as the basis for the next message, thereby eliminating the need to retype the fill-in repetitive information.

### **35 Deferred Messages**

Once a completed message is on the screen, the user has the option to automatically send it at any future time. This future time can be minutes, hours, days, etc into the future. The user is prompted to enter a specific time-of-day and a specific date. The default values in the dialog box are for the following day at 6 minutes past midnight. This default time can be set as a configuration parameter.

### **36 Keyboard Macro Facility**

A keyboard macro definition file defines sequences of text characters that are inserted whenever the corresponding key or key combination is typed. For example, an address list of up to 8 addresses, or a complete 1,800 character standardized message, can be inserted by a single keystroke. Also, a formatted table of multiple rows and columns can be defined as a keyboard macro. The keyboard macros can also be used to automatically fill in fields within a message template.

### **37 Automated Dial Backup Configuration for Concentrator Sites**

For those concentrator sites that do not handle heavy traffic loads, it is possible to reduce costs by using only a single WAN link and router and provide backup via an automatically dialed-up voice telephone line to the switching center. The dial-up service is provided by ordinary low cost industry standard V.90 modems. The dial-up function can also be used to offload high message queues on the FEP router port. Since the voice telephone network itself provides a great deal of resiliency, it is even possible to connect a concentrator site to the switching center by **only** a dial-up line. Whether this dial-up only connection between the concentrator and switching center is cost-effective depends upon the combination of traffic load and toll call charges in effect. Since calls only last for the duration of the accumulated message traffic transmission time, this method is typically viable for any node that handles fewer than 500 daily messages.

Messages are batched on both the switching center and FEP sides, and up to 300 messages will be delivered, in either direction, during a single call. Calls are automatically generated at a rate based on a combination of lapsed time and accumulated messages. This provides a reasonable compromise between telephone toll call charges and user-settable tolerable average message delay of 1 minute. Based on the local tariffs there is always some point of traffic load increase at which the toll charges

amount to a higher cost than a dedicated line. If that point is reached, then a router must be installed and the FEP routing tables changed accordingly in order to minimize operating costs.

### **38 Automated Dial-Up Message Service for End-Users**

By using ordinary V.90 modems on the voice telephone network, authorized end-users, such as regional airports, weather observation stations, etc., can send and receive message traffic over calls between the end-user and either the switching center or the concentrator site. Connecting to the concentrator site minimizes any possible long-distance call charges. Various security techniques are employed to preclude unauthorized users gaining access to the AFTN network. This option provides a very low-cost means of connecting all of the regional airports, or any other authorized users, to the AFTN network. The ACK/NAK error correcting protocol insures at least 45 attempts, per message, to transfer the message error-free. To minimize call-blocking and continuous busy signals, at least 2 switching center telephone numbers should be available to the end-user. As the number of dial-up users increase, the number of dial-up lines at the concentrator sites must be expanded to insure quality of service.

The AFTN operational staff can determine which dial-up numbers are provided to which users. The assigned numbers can be changed easily by using a text editor on a dial-up routing file. In order to insure network security, these numbers will be invisible to the user and automatically dialed by the MMS terminal program. An automatic password is exchanged at least daily and the password is randomly changed at least once per day. In addition other proprietary security techniques are used to protect against Denial-of-Service (DoS) attacks and message spoofing. If either DoS or message spoofing attempts are detected, a descriptive alarm message is automatically sent to the operator alarm position.

### **39 Unattended Operation Parameter**

The 'unattended operation' option checks a circuit parameter to return any message containing a format error to the source of the message. A copy is sent to the system Reject position, where it is eventually deleted after a user-settable lapsed time period. The message returned to the source is encapsulated and a detailed plain language error message is appended.

Also, a user selected remote terminal sends a message to itself every 5 minutes. If 7 minutes passes without a returned self-addressed message, the terminal notifies a monitoring station every 3 minutes until service is restored. This monitoring station can be either a direct connected terminal or a dial-up connection.

Also, any abnormal condition, such as a high message queue, or a route failure not covered by the automatic alternate routing described in section 9, invokes a customized script which executes alternate routing or hold commands. The event-triggered script carries out exactly the same commands that would otherwise be prescribed for an on-site operator to carry out. When the abnormal condition is cleared, another specific event-triggered script is executed to return the system to the state that existed prior to the abnormal event.

## 40 Contingency System Option

The contingency system provides a fully-equipped second switching center at a location physically remote from the main switching center. Although the 2 switching centers may very well be hundreds of miles apart, they are both connected to the same WAN. Also, all of the remote concentrator sites that are also connected to the common WAN can send their messages to either or both switching centers. Both of the switching centers each provide over 99.999 % availability. This contingency system option is typically required where the AFTN generated revenue must be protected by commercial insurance. To minimize the otherwise very large insurance premiums, a contingency system insures that no catastrophic event, such as flood, fire, explosion, etc., can cut-off the AFTN service for even a very brief period. Note that the contingency system is **not** used at all for normal operational backup, since the main switch is totally protected against a total system failure, based on its own distributed architecture.

The FEPs at the remote concentrators can dynamically adjust to a change in 'on-line' system and 'hot-standby' system assignments, in reaction to commands sent out by either site. Under operator control, the FEPs send the message traffic **either** to both sites, or only the current on-line site. Traffic received by the 'hot-standby' site is routed in the same manner as the on-line site. However, except for certain special cases, the hot-standby site skips the very final step of actually sending out the resulting messages through its attached WAN routers. The role of 'on-line' and 'hot-standby' site can be switched under operator control at any time from either site. An alternate routing command executed at one site, is automatically passed to the other site for execution. Normally, the 'hot-standby' site is totally unmanned, and will operate indefinitely in parallel with the on-line site.

## 41 NOTAM Handling Option

A complete automated NOTAM facility based on a mirrored SQL data base can be provided within or outside of the AFTN switching center. However, this option relates to a more limited non-SQL data-base function, which can be utilized as a supplement to an existing NOTAM facility, or a limited automated implementation of a NOTAM handling facility. As in the case of the AFTN Contingency System in section 39 above, the NOTAM function can be replicated in one or more duplicated remote locations. In this case all duplicated NOTAM systems receiving incoming messages but only the on-line NOTAM system generates output messages.

All of the normal functions listed in Annex 15 can be carried out by this option, within the AFTN system. The function provides for the automatic replacement or cancellation based on the NOTAMR and NOTAMC messages. A NOTAM message template is provided to facilitate NOTAM origination. A format and 'reasonableness' validation check is performed on any message entered for storage or presented on the screen for transmission. Multi-part NOTAMS can be assembled or disassembled by a simple operator command.

In addition to the NOTAMC means, the user can optionally establish a time limit in which the NOTAM is automatically removed. In addition to retrieval by NOTAM serial number, NOTAMs can be retrieved by **any** contained text. Up to 400 addressees can be invoked for any single NOTAM transmission.