WG2/WP____
JSG/WP____

ATNP JSG/WG2
Utrech, Netherlands
26 June 1998 – JSG
29 June-1 July1998 – WG2

IATA Expectations for Remotely Managing Airborne Resources

Presented by Paul Hennig

Summary

Attached ATN Systems, Inc. (ATNSI) document titled ATN Network Management Concept of Operations contains text on IATA Expectations for Remotely Managing Airborne Resources. IATA is pleased to answer questions and/or provide additional documentation.

1. Introduction

At the March 1998 Rio meetings, IATA agreed to provide Working Group 2 and the Joint Subgroup on System Management with information on how airlines intend to manage their airborne ATN resources.

The attached ATN Systems, Inc. (ATNSI) document titled ATN Network Management Concept of Operations, Version 98.0.5, dated May 1998 contains text on the subject. The document is work-in-progress, with the expectation of a September 1998 completion date.

2. Proposal

The groups are invited to review the attached document, particularly Section 3.2.1. IATA will be pleased to answer questions and/or provide additional information.

ATTACHMENT-1

ATNP WG Meetings
Rio de Janeiro, Brazil
March 1998

ACTION ITEM 14/6: Mr. Hennig to provide input to next WG2 meeting on IATA expectations for remotely managing airborne resources.

WG2/14 FLIMSY 3.2
WG3/12 FLIMSY 1.2
17 March 1998
Rio de Janeiro, Brazil

JOINT WG2/3 FLIMSY
SYSTEM MANAGEMENT RESOLUTIONS AND ACTION PLAN

1. Any managed object (MO) deemed important enough to be detailed in either SARPs or Guidance must be defined using GDMO to assure interoperability. This applies regardless of whether or not any particular MO is specified to be exchanged across administrative boundaries (manager-manager or agent-manager).

2. A baseline managed object containment tree has been proposed. Between Rio and Utrecht, WG2 and WG3 system management experts will review the proposed MO containment tree for format and content, focusing on the subtrees in their areas of expertise. The goal is an agreed-to MO containment tree at Utrecht.

3. Another goal for Utrecht is identification of at least one (1) managed object (MO) which all States and organizations agree to share, agent-to-manager or manager-to-manager. If at least one (1) MO cannot be identified and agreed to by Utrecht, then all system management material may only be Guidance unless "health of the system" suggests SARPs are necessary for what, in essence, is a local matter.

4. IATA will present a paper at Utrecht explaining how commercial airlines intend to manage their airborne resources.

ATTACHMENT-2

ATN Systems, Inc.

ATN Network Management Concept of Operations

Version 98.0.5
May 1998

This working paper is an interim draft of the ATN Network Management (NM) Concept of Operations (CONOPS) currently being developed by the ATNSI Network Management Task Force. The NM CONOPS will define the concepts and address the issues involved in managing an ATN network across multiple domains in a global CNS/ATM-1 environment.

Prepared By:
The ATNSI Network Management Task Force and
The MITRE Corporation

1820 Dolly Madison Blvd.
McLean, VA 22102
For:
ATN Systems, Inc.
1215 Jefferson Davis Highway
Crystal Gateway 3 - Suite 1010
Arlington, VA. 22202
v: 703-412-2900 f: 703-412-2906

REVISION HISTORY

Revision	Date	Author	Comments
97.0.1	September 1997	Taylor	Initial draft outline presented to ATNSI
97.0.2	October 1997	Taylor/Laqui	Second draft outline based on comments from airlines
98.0.2	January 1998	Laqui	Release for comment and development into NM CONOPS by ATNSI NM Task Force
98.0.3	March 1998	NMTF, various	Revised draft with contributions from NMTF and further development by ATNSI. Released for comment and continued development.
98.0.4	April 1998	Editors	Revisions in progress.
98.0.5	May 1998	NMTF, various	Revised draft with NMTF contributions to Section 3, further development of Section 3 and 4 by ATNSI.

Keywords:

ATN Network

Network management

Systems Management

Service Level Agreement

Executive Summary

To be provided

Table of Contents

LIST OF FIGURES:

Section 1

Introduction

The Aeronautical Telecommunication Network (ATN) is a world-wide data network intended to support data communication connectivity among mobile platforms, airlines, government authorities that provide Air Traffic Control (ATC) and Flight Information Services (FIS), and other companies that provide services such as Aeronautical Operational Control (AOC), Aeronautical Administrative Communications (AAC), and Aeronautical Passenger Communications (APC). This network is being designed as a collection of dissimilar transmission networks and interconnecting computers that will operate as a single, cohesive, and virtual data network. The goal is to provide full and flexible support for data communications among aviation users and Air Traffic Service (ATS) providers around the world, both fixed-base and mobile.

The ATN is based upon standards and guidelines from the International Civil Aviation Organization (ICAO). These standards and guidelines are, in turn, based upon the Open Systems Interconnection (OSI) protocols formulated by international standardizing bodies such as the International Organization for Standardization (ISO).

ATN routers are the primary elements of the internet portion of the ATN that are used to interconnect local data networks to enable data exchange for the ATN aviation applications. The ATN routers will be owned and operated by multiple global organizations such as Civil Aviation Authorities (CAAs), aviation communication service providers, and airlines. To achieve a seamless, transparent data communication service, global coordination of the management of the ATN internet is essential.

1.1 Purpose and Scope

The purpose of this Concept of Operations (CONOPS) is to define the basic concepts of how organizations will coordinate and cooperate in providing network management to the operation of the ATN.

ATN systems management provides for deterministic and controllable behavior in support of the required communications service levels by providing facilities to control, coordinate, and monitor the resources that allow communications to take place in the ATN environment. This CONOPS addresses ATN network management, which is the set of functions related to the management of the ATN resources and their status.

This CONOPS addresses global network management issues specific to international air/ground (A/G) and ground/ground (G/G) communication operations including cross-

organizational issues among Civil Aviation Authorities (CAAs), airlines, and ATN service providers.

This CONOPS identifies the organizations participating in the ATN, their roles and responsibilities for ATN network management, and the interactions that are expected to occur among the organizations in the international environment.

Network management issues that impact the overall service quality of ATN include:

- Global service quality uniformity and user expectations.
- Management information exchange across organizations for ensuring performance of the overall network and for enabling proactive maintenance.
- Seamless management of connectivity for transparent hand-off of A/G and G/G communications between domains.
- Data management and ownership.

These issues are addressed from an overall integrated network management perspective. A target operation environment is briefly described to direct evolutionary efforts. Based on the target operation environment, near term i.e., “Day1”, ATN management is discussed. target operation environment serves as a reference goal for discussion of Day1 and subsequent ATN environment so as to achieve fully integrated management.

Because the global adoption of the ATN will be an evolutionary, incremental process, this version of the CONOPS concentrates on a limited operational environment, “Day1," as a starting point.

The Day1 ATN is defined as the operational state of the ATN when the first commercial aircraft enters revenue service equipped with and using data link for Airline Operational Control (AOC). The Day1 aircraft may also be certified to use the ATN infrastructure for Air Traffic Control (ATC) data link.

1.2 Motivation and Task Background

The ATN is a component of CNS/ATM that serves as the communication infrastructure for different A/G and G/G ATM and airline applications. Management is necessary to ensure a level of service consistent with the certification and safety demand of global ATM for the community to receive operational benefits of ATN.

In addition, the large-scale structure and distributed nature of the ATN environment with multiple administrators, institutions, and end users, makes the need for coordinated network management efforts imperative.

This CONOPS originates from the need to understand the level of coordination required to ensure ATN network (internet) operation, and to establish a common goal for refining the

detailed concepts for ATN network management. This document addresses ATN network management needs in a top-down manner and is intended to be complementary to other ATN network management studies.

This CONOPS is a product of a team of representatives from commercial airlines, CAAs, service and network providers, and standards organizations. Information from other ATN management studies serve as references to this document when appropriate.

1.3 Other ATN Management Activities

1.3.1 ATN Management in the Context of the ProATN Project

The ProATN Project aims to develop a Managed prototype ATN CNS/ATM-1 Package. This Prototype ATN will contain pre-operational, pre-industrial, and certifiable End Systems (ES) and Boundary Intermediate Systems (BIS) which will be managed by experimental Network Management Stations.

The ProATN Project is executed by the ProATN Consortium, consisting of 16 European industry, research, and Civil Aviation Administration (CAA) partners. The project is funded jointly by the European Commission, EUROCONTROL, and the ProATN Consortium.

The ProATN Network Management Stations and Network Management Agent are planned to conform to the Systems Management draft Standards and Recommended Practices (SARPs) that are currently being developed in ICAO.

The ProATN Network Management Stations will be developed in the context of the ProATN Project itself. The Network Management Agents (NMAs) of the ProATN End Systems and Boundary Intermediate Systems are intended to be provided by the industrial company that is developing the NMAs for integration with the Router Reference Implementation (RRI) and the Application Service Elements (ASEs) for the four air/ground applications of the CNS/ATM-1 Package which it is also developing. Task Teams are established with participants of relevant parties to coordinate activities to ensure manager-agent interoperability and conformance to the draft ICAO SARPs.

The ProATN Prototype Infrastructure is intended to be operational by the end of 1999. However, several elements of the Network Management infrastructure are expected to be available earlier.

1.3.2 ATN Management Activities Within AEEC

The Airlines Electronic Engineering Committee (AEEC) has formed a working group to prepare a specification on the airborne aspects of systems/network management for the ATN. This work leverages the ATN SARPs and Guidance Material (GM) adopted by ICAO, adding critical detail for avionics developers (i.e., matters usually left to local implementation).

1.3.3 ATN Management Activities in ICAO

The ICAO ATN Panel (ATNP) is currently in the process of defining the System Management Standards and Recommended Practices (SARPs This effort is directed towards investigating the management requirements for the ATN Internet, Upper Layer, and Application SARPs but it is not addressing issues relating to the management of resources supporting those communications. The SARPs will define the protocols for use in exchanging management information and the minimum set of Managed Objects (MOs) required.

The current schedule is for the ATNP to have completed its work on the SARPs before the next Panel meeting scheduled in December 1999. To meet the schedule, drafts of the ICAO CONOPS as well as initial definition of the management protocol structure will be completed before the end of 1998.

1.4 Benefits of this CONOPS

This CONOPS is a benefit to the ATN community in that it:

- Reflects the concerns of airlines, ATN service and network providers, and CAAs.
- Provides realistic concepts for coordination of the management of ATN networks.
- Addresses issues and identifies needed standards for ATN network management capabilities.
- Coordinates engineering efforts in achieving integrated network management for the ATN.
- Identifies network management interfaces to other subnetworks in the aviation industry.

1.5 Document Organization

This document is organized as follows:

Section 1 Introduction

ion 2 Background -- Describes potential ATN environment and establishes the basis for describing overall institutional network management issues.

ion 3 Management Concept -- Describes an ATN network management concept by specifying the organizations, their roles and responsibilities, and their network management interactions in the ATN environment.

ion 4 Operation Functions -- Specifies guidelines for network management service agreements or contracts between the organizations for establishing integrated management efforts in the global ATN environment.

ion 5 Conclusion -- Summarizes the network management concept described in this document.

Section 2

Background on ATN Network and Network Management

This section provides a brief overview of the ATN to establish the context and to clarify the common terminology used. It describes the ATN capabilities and provides scenarios for network and the network environment of the ATN as it is anticipated to be in Day1 operation.

This section introduces the basic concepts of the network management processes and functions and identifies the network management information to be exchanged across organizational boundaries in preserving global quality.

2.1 ATN Background

As specified in Section 1, Introduction, the ATN is a global telecommunication network that spans organizational and international boundaries and provides a common communications capability for Air Traffic Services (ATS), ATM and airline applications, and aviation industry applications that require G/G or A/G data communications.

The ATN utilizes existing communication subnetworks and infrastructures wherever it is possible and feasible. The ATN offers various Air Traffic Services Communication (ATSC) classes and operates in accordance with defined communication priorities to satisfy the security and safety needs of the aeronautical users.

Where appropriate standards and practices existed, they were adopted and incorporated into the network architecture. To define the elements of a complete network architecture, special modifications and enhancements to accommodate the unique requirements of the evolving aviation environment were added by ICAO panel experts.

The ATN introduces the following features to aviation communications:

- High-speed, packet switching networks with dynamic routing capabilities.
- Extension of the functional network to include A/G links using a variety of subnetworks.
- Mobile subnetworks comprises aircraft ATN intermediate systems.
- Data communication services and application entities that support end-to-end delivery of ATS and other aviation applications.

ATN Network Management will accommodate:

- Dynamic management and control of numerous network elements on a world-wide basis.
- Modern communication technology.

- The demands and expectations of a rapidly expanding world-wide user community of aviation interests, that includes CAAs, airline operators, and communication service providers.

2.1.1 ATN Architecture, Topology and Functions

This section provides a description of the end-end ATN data network. The ATN is partitioned into its component subnetworks for discussion of network management.

Figure 2-1 presents a composite of all the elements of the ATN. The bottom of the figure illustrates ATM and airline applications providing services via the ATN internet. The ground internet maintains connectivity by means of A/G subnetworks with aircraft equipped with avionics that support an airborne subnetwork connected to an on-board ATN router. End-to-end ATM and airline application services are indicated by lines with double arrows.

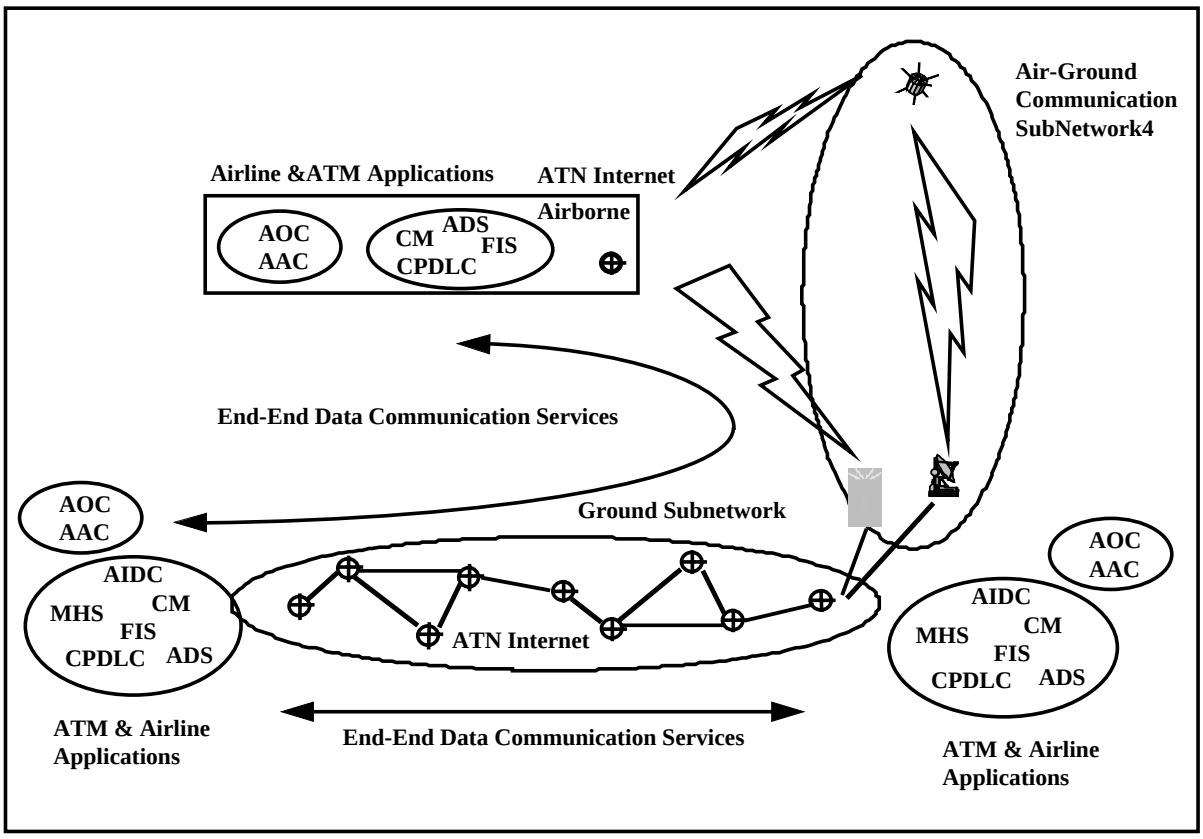

Figure 2-1 ATN Components

2.1.2 Protocols and Routing

Figure 2-2 presents a schematic view of the essential elements of the ATN. Using combinations of these elements, the ATN will operate in a multinational communication environment with different communication service providers. This is made possible through the interconnection of common elements designed to conform with the ICAO SARPs.

The scope of this Network Management CONOPS focuses on the distributed nature of the ATN Internet.

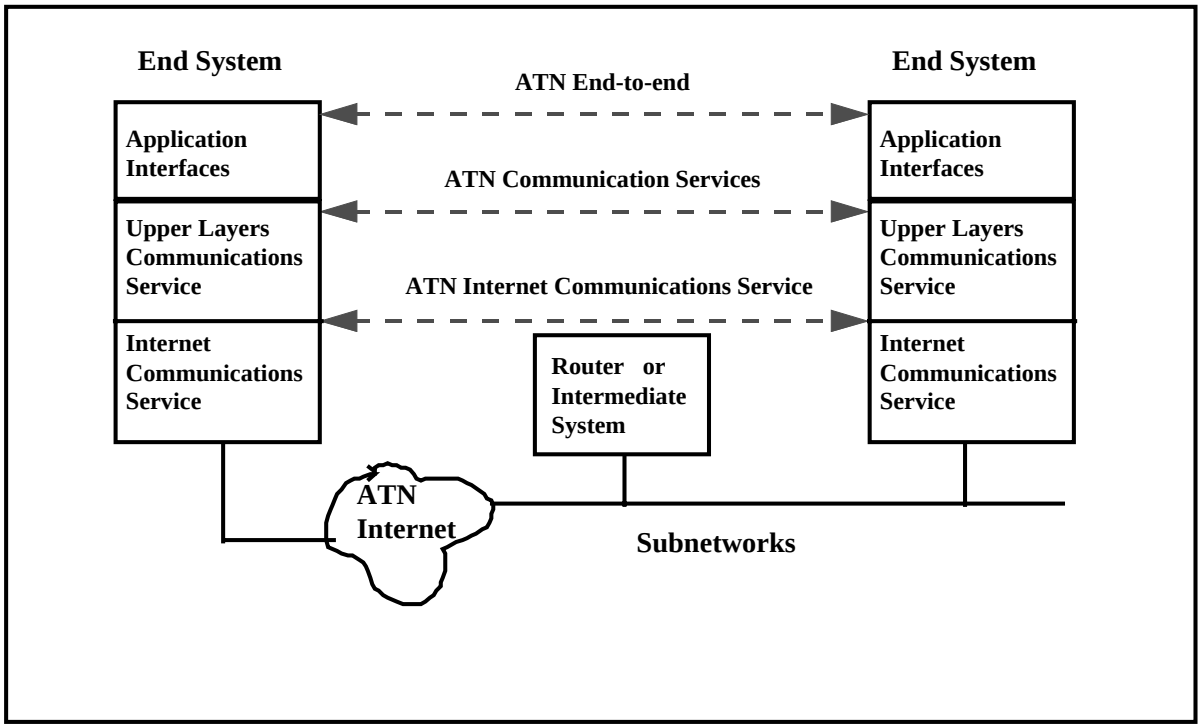

Figure 2-2 Essential Elements of the ATN

2.1.3 ATM and Airline Applications

The ATN includes aeronautical applications that rely on the ATN network and provide information services to all segments of the aviation industry.

ATM and Airline applications that are currently planned include critical applications for Air Traffic Control (ATC) and for the Flight Information Service (FIS): Controller Pilot Data Link Communication (CPDLC), Automatic Dependent Surveillance (ADS), Air Traffic Services Interfacility Data Communication (AIDC), Context Management (CM), Air Traffic Service Message Handling System (ATSMHS), and Automatic Terminal Information Service

(ATIS). Airline applications (AOC and AAC) will share A/G subnetworks with ATM applications. Value-added ATM applications for AOC and APC will also be developed.

To ensure high quality service delivery, exchange of management information between ATN internet, the A/G subnetworks, and applications (application processes) is strongly - desirable. Suggestions for this type of information exchange are discussed in this document.

2.1.4 Day1 Operational ATN

For the purpose of this CONOPS, the Day1 operational ATN is the operational state of the ATN on the day that the first commercial aircraft is certified to use Airline Operational Control (AOC) or Airline Administrative Communications (AAC) data link applications over an ATN infrastructure. The Day1 aircraft is likely to support the limited (PETAL II) CPDLC message set installed in their communication management units (CMUs) for use in CPDLC Build-2 as in the PETAL II and/or FAA Flight 2000 (F2K) trials. The Context Management (CM) application will also be necessary for these trials. Day1 aircraft will employ the VDL MODE 2 A/G subnetwork and the SATCOM DATA 3 A/G subnetwork. The current expectation is that most USA airlines will forward/retrofit all their old technology ACARS aircraft in five to seven years from start of operational ATN service.

This CONOPS acknowledges that the very first operational use of the ATN is expected to be the USA/Japan ATN G/G link for ATSMHS as replacement to current AFTN capability.

2.2 ATN Network Management Environment

Management of the ATN network entails coordination among the management functions of the ground ATN internet, A/G communication subnetworks, and the airborne ATN internet. In the near term environment, additional coordination with the management of existing data networks is necessary to ensure end-to-end connectivity and delivery of services to ATM and airline applications. From an ATN network management perspective, the service provided by the network portion of the ATN is the capacity for end-to-end communication for the ATM and airline applications. The actual physical connectivity is a network function and not a network management function.

The distinction between the management of the ATN network and the management of the end-to-end ATM and airline applications that use the network portion of the ATN is that the latter also includes the management of the application processes besides the communication layers. The content of data flowing through the ATN is transparent to ATN network management. An application error or failure is not detected by the ATN network management but by the ATM and airline application management. ATM and airline application management is responsible for ensuring that an application is performing its functions and of the accuracy of the information shared in application exchanges.

Management of the communication network, that is, the ATN internet, A/G communication subnetworks, or other interconnected data subnetworks, encompasses the controlling, monitoring, and maintaining of the network elements that make up the network.

The current aeronautical data networks are owned and maintained by different organizations. Similarly, the global ATN network comprises different segments that are owned and maintained by different organizations. To ensure that the ATN network is providing seamless global end-to-end connectivity and timely delivery of application data, the different segments of the network must operate according to their respective performance criteria. Failure in a segment of the network may affect the performance of neighboring segments or the entire network. Coordination is necessary to maintain the entire network at an acceptable level of performance.

The ATN router in an aircraft is an avionics device that must meet maintenance and airworthiness certification requirements. It is assumed that airlines are responsible for the management of the airborne ATN subnetworks in the aircraft they operate. For General Aviation (GA), the owners of the aircraft are responsible for avionics maintenance and certification including correct configuration and handling of fault and performance data.

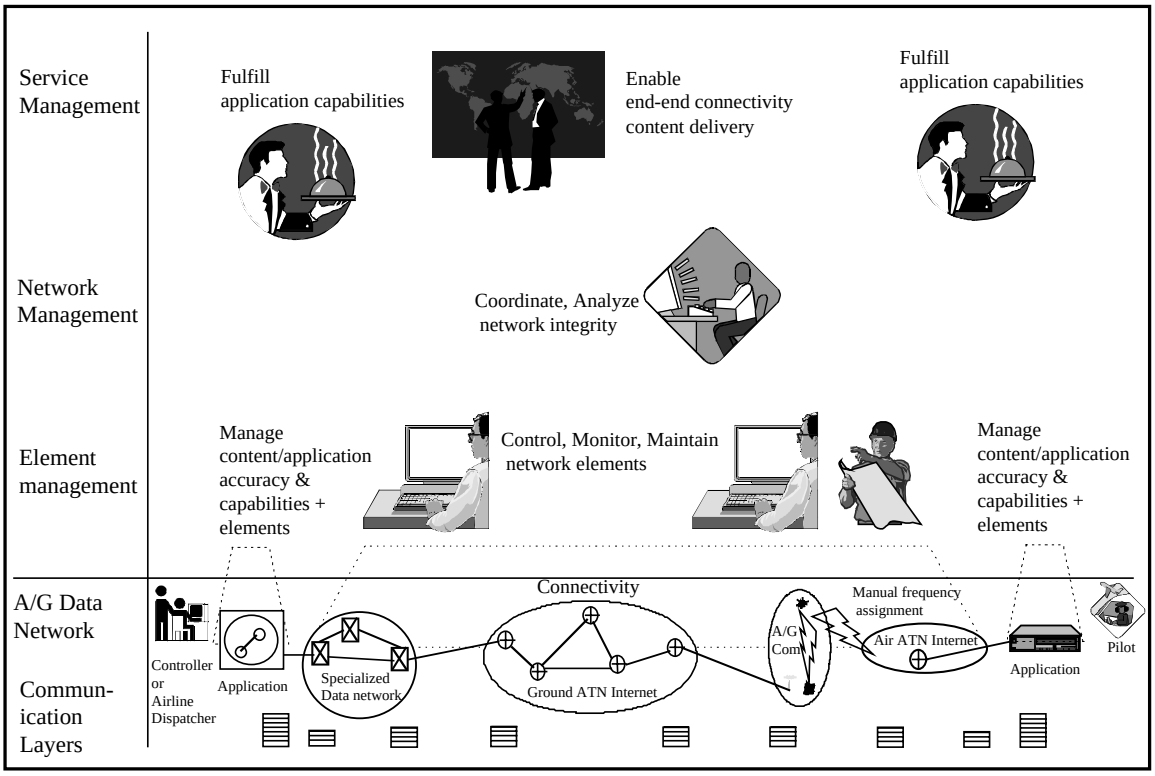

Figure 2-3 Network Management Responsibilities

2.2.1 ATN Network Management Architecture

An organization is likely to own and maintain multiple ATN subnetworks or segments that are not adjacent to each other. These segments could be managed under one management domain or as separate management domains based on the operating goals of the organization. Management domains that share the same goals are considered to be within the same administrative domain. Administrative domains could also be composed of management domains that belong to different organizations because of economic or political arrangements. European CAAs and EUROCONTROL may together form such an administrative domain, for example.

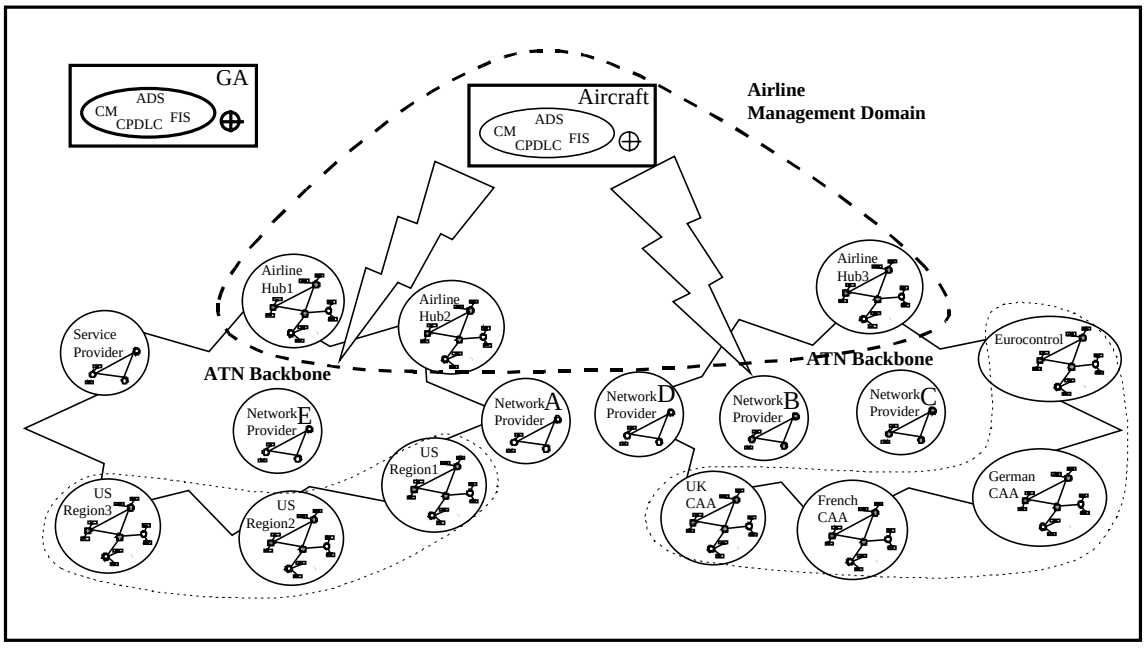

Figure 2-4 Participants in the ATN Community

An organization or administrative domain may adopt a hierarchical management structure to distribute the various network management functions. For example, an organization may adopt a three–tier management hierarchy wherein tier 1 is composed of network operators who control, monitor, and maintain the ATN network elements along with other subnetworks. Tier 2 may integrate and correlate network element information to manage from a regional perspective. Tier 3 may coordinate from the national level. The network management structure is based on operational or economic needs. It is not necessary to impose a uniform network management hierarchy for all organizations or administrative domains for them to effectively cooperate and coordinate in management of the global ATN.

A practical and flexible approach for establishing network management coordination is to model the existing operations. Two organizations engaged in communication exchanges

establish a service level agreement between them and explicitly state their expectations for the common endeavor. The agreement is enforced by both organizations. When there is a change in operational needs, re-negotiation of the agreement can be readily performed. An organization may have several bilateral service level agreements established with multiple organizations. The intent is to achieve global network management coordination via the chain of bilateral service level agreements between participants of ATN.

To establish meaningful and effective global network management coordination, procedures for bilateral service level agreements need to ensure that mission-critical aspects of network management coordination are completely addressed. The components for establishing service level agreements include identifying the organizations, their responsibilities and roles, the network management interactions among them, and the overall network management processes and functions. These are discussed throughout the rest of this CONOPS.

2.2.2 Network Management Processes

This section examines network management scenarios for ATN to identify areas that require cross-administrative domain interactions. These case studies include typical generic scenarios and some ATN specific scenarios. The case studies are presented as ATN network management processes and are described in generic terms to provide a common reference for discussion. To examine network management interactions among organizations, these scenarios are centered on key roles in the ATN community. Network management functions performed within an organization may be outlined for the continuity of the case study. Variations in network management processes within each domain are expected, however. The case studies indicate expected management functions and responsibilities for a given role. These functions are discussed further in sections 3 and 4.

For ease of understanding, the processes are discussed under the five standard management functional areas. They are: Configuration, Fault, Performance, Accounting, and Security management.

2.2.2.1 Configuration Management Process

Although planning for network management is an integral part of network planning and engineering, this section considers the main network management processes that begin after the network is installed.

In Figure 2-5 the shaded areas indicate the network function tasks that are undertaken to establish and configure the network.

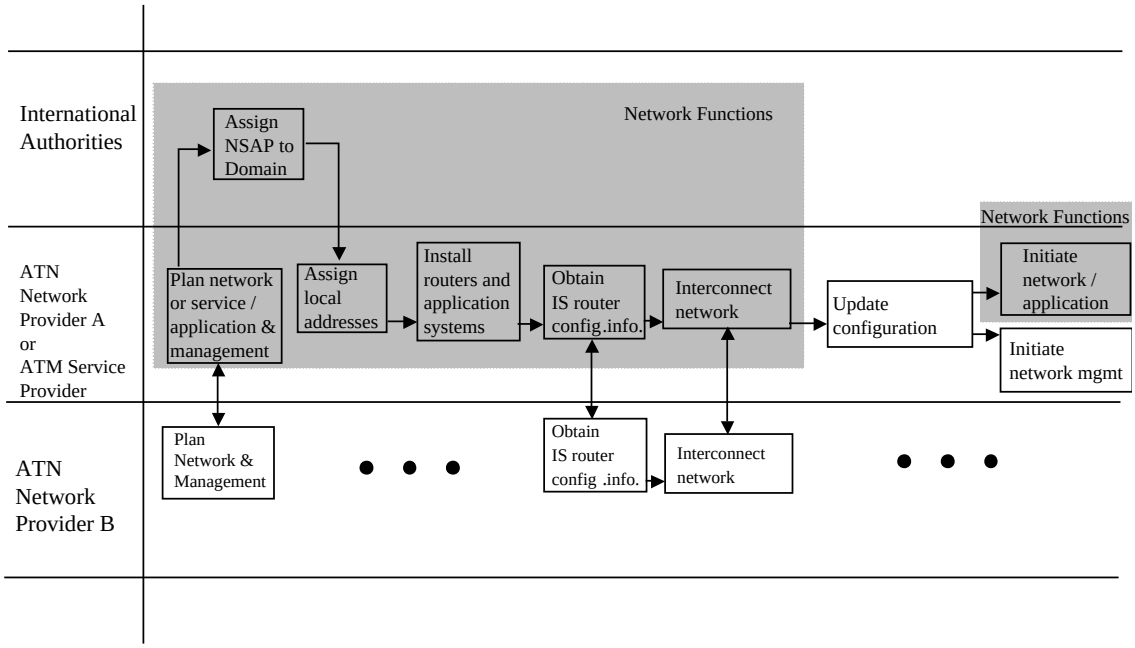

Figure 2-5 Configuration Management Process - Initiate Network Management

In Figure 2-5, an ATN network provider “A” plans and engineers a portion of the ATN. A Network Service Access Point (NSAP) address is obtained from the appropriate authorities (ISO, ICAO, or the International Air Transport Association (IATA)). Once the network is installed and ready to provide services, configuration information and other pertinent network information are recorded and provided by the network engineers to the network management operators. Assignment of local addresses may be a joint effort between network engineers and network management operators if higher level authorities have ceded responsibility over one or more of the address fields higher than the Transport Selector (TSEL).

ATN network provider “B," in Figure 2-5, engages in the same process and exchanges configuration information with network provider “A."

Typically tier 1 network operators are responsible for administrating network and configuration information. Changes to configurations can occur for reasons given in the following scenarios:

1. Expansion of the network with new network elements being added
2. Improvement of the network based on performance analysis
3. Interconnection with (ground) service providers or other network providers
4. Preparation for recognizing airborne ATN routers

5. Network reconfiguration due to element failure
6. Network reconfiguration due to a routing policy change
7. Re-initialization of network for disaster recovery

In scenario 1, the configuration change process is generally within a management domain except when a BIS is introduced. In this case, configuration information is exchanged between management domains and coordination is needed. Most of the functions for this case are likely to be performed by network engineers. For example, to certify interoperability of equipment and handle other network interconnection issues. The management functions performed in this process involve accepting the configuration information of the new system and propagating the information within the network when appropriate. Cross-domain management interaction is insignificant in this scenario.

In scenario 2, performance analysis results may come from network engineers or network management analysts. It may also result from analysis provided by sources outside the organization. Once the results are accepted, network management operators schedule and change all affected network elements. Depending on the degree of change, neighboring domains may be affected and coordination is necessary. Analysis results, as well as configuration change information, may need to be shared across domains.

Scenario 3 is similar to the special case in scenario 1 where the network engineers perform most of the functions in this configuration change process.

Scenario 4 is similar to the special case in scenario 1 where the network engineers perform most of the functions in this configuration change process.

Scenario 5 is most likely within a management domain that has little or no cross domain management interactions.

Scenario 6 addresses configuration changes that are time sensitive and require coordination among the affected organizations. The organization that initiates the policy change identifies all the affected organizations. Negotiation and agreement on the changes determines the configuration change data. The initiating organization verifies the configuration change data and disseminates the data to all the affected organizations. Because policy changes need to be implemented by a certain time to take effect electronic dissemination of the data is desirable. This type of exchange is preferred to a network manager to cross domain network manager procedure. Within a management domain, network management operators schedule off-peak time to configure the network elements within their domain. Once the work is completed, the initiating organization is notified.

Scenario 7 is for addressing catastrophic network failures due to uncommon events such as natural disasters. Typically an organization implements its own disaster recovery plan. However, agreement between different administrative domains may be established to minimize regional impacts.

Summary of the configuration management processes

Based on the above scenarios, the characteristics of configuration management process are as follows:

1. Configuration changes in the ATN ground network are time sensitive and need to be in effect by a deadline. However, interactions among organizations are mostly non real-time. No immediate action nor direct flow of changes from cross domain network manager to agents has been identified.
2. Configuration changes typically affect services and are performed at low-peak hours within a domain. For the global ATN network, low-peak hours will differ from region to region. In coordinating configuration changes, sufficient time is needed to allow the affected organizations to implement the changes.
3. Configuration changes are likely to affect more than one router. To avoid long down times for upgrading the configuration and for reducing errors in propagating the changes, automation within a domain is desirable.
4. Configuration responsibilities are often shared between network engineers and network management operators. Within a domain, it is expected that coordination between the different functional groups will be encouraged to ensure the continued ATN network operability.
5. Configuration changes of BIS routers and routing policies need to be coordinated among all the affected organizations. Changes and schedule need to be agreed upon before they are put in effect.
6. A suggested process for coordinating configuration changes is as described: An organization determines if an ATN network configuration change will affect other organizations. If it will, the initiating organization submits a change request to the affected organizations. The change request includes the proposed changes, the reasons for the change, and the desired effective time. Each recipient organization, through its internal processes, evaluates the request and responds to the initiating organization. To reject a request, the response should include the reasons for the rejection and proposed modifications to the proposed change. In the case of acceptance of the request, a commit time for implementing the change is provided. The initiating organization evaluates the responses and takes the appropriate action to resolve any differences with individual organizations. Once finalized, the initiating organization sends a confirm change request to all the affected organizations. In the case where a change request is aborted, a cancel request is sent to all the affected organizations. Upon completion of the changes, the affected organizations are required to notify the initiating organization of the status. The initiating organization closes the change request and posts the status to the affected organizations.
7. The process described in 6 assumes that the changes are within the standards for ATN

router performance, that is, even if a portion of the ATN network cannot implement the change request, the performance of the entire ATN will not be not severely affected. For a change in ATN network performance criteria, the process for amendment involves going through a standards review procedure.

8. The affected organizations are likely to be those with SLAs with the initiating organization. Each affected organization evaluates and determines the impact on its partnering organizations of the configuration change. The affected organizations in turn initiate configuration change request to their partnering organizations that are also affected by the change.
9. Every organization is expected to backup configuration information and to keep it at a physically separate location. Each organization must have a disaster recovery plan in case of catastrophic failures. The recovery plan needs to be understood by all responsible personnel. This includes periodic drills to familiarize and prepare personnel to handle the disaster situations.

2.2.2.2 Fault Management Process

Once the network is in place and operational, maintenance of the network is initiated. Fault management begins with updating the network topology, and establishing the schedule for monitoring the network for events or alarm notifications.

A network fault may be detected by inputs from several sources.

1. Alarm notifications generated by network elements
2. Customer complaints
3. Reports from adjacent networks

Source 1 typically comes from monitoring within a domain with no exchange with other management domains. However, if a problem can affect a multi-domain service, the other domains may need to be notified as in source 3, below.

Sources 2 and 3 are external feedback into the management domain. In source 2, the typical means are telephone calls or electronic messages where customer contact personnel interact with the customers. For source 3, reports may be via exchange of electronic trouble tickets if a bilateral agreement is established.

Regardless of the sources of fault reports, the process for handling each fault is similar. This is illustrated in Figure 2-6 and Figure 2-7.

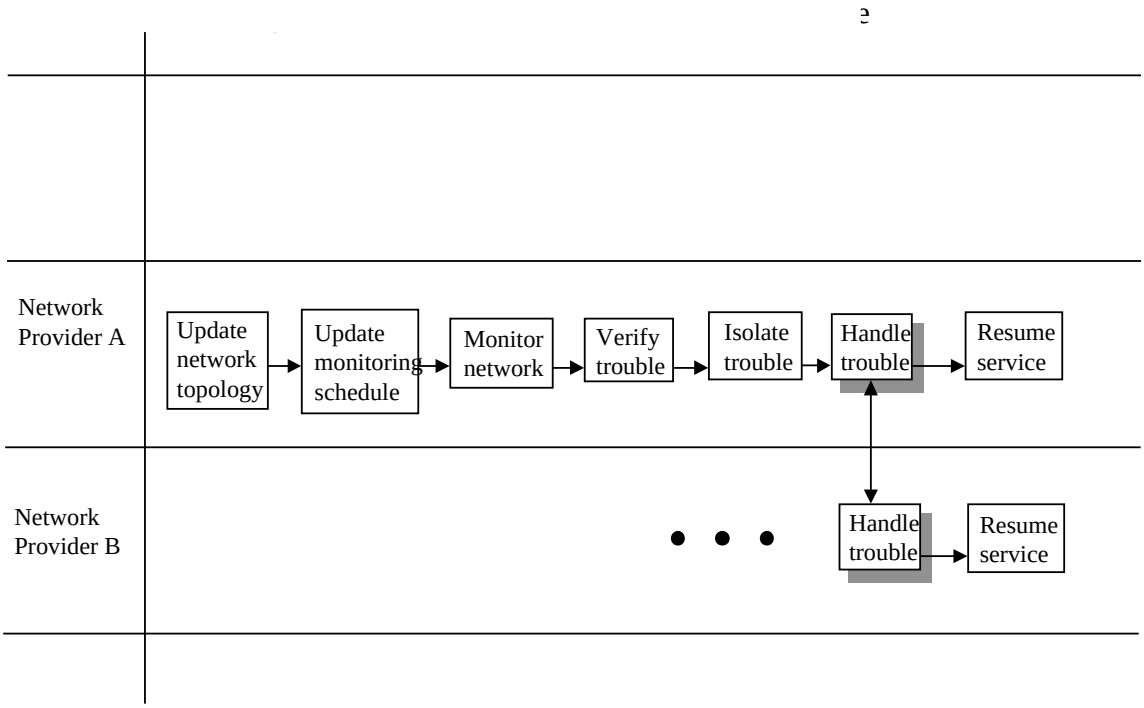

Figure 2-6 Fault Management Process (1) - Initiate Maintenance

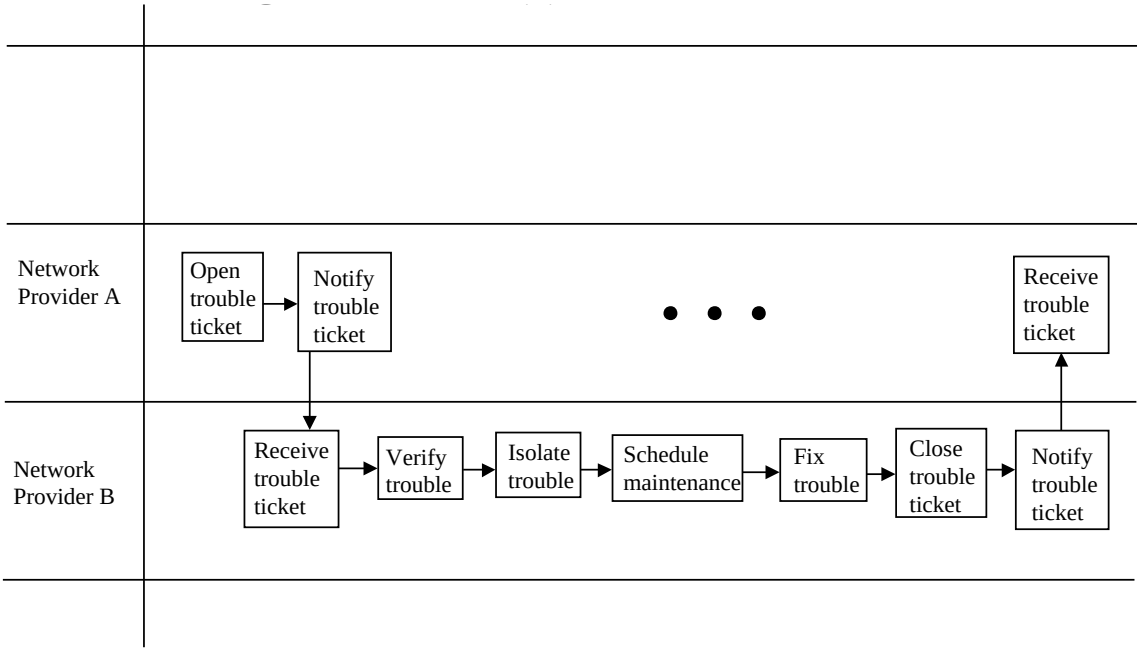

Figure 2-7 Fault Management Process (2) - Handle Trouble Ticket

Figure 2-7 illustrates a fault scenario where a network fault that originates outside the management domain of a network provider is detected. The fault is reported to the domain where the fault resides for mitigation.

From end-user to end-user, faults in the different segments of the network will have impacts on end-end services. These segments are:

1. Ground application errors
2. Data network errors
3. Leased line network errors
4. A/G network errors
5. Airborne network errors
6. Airborne application errors

These segments are all illustrated in Figure 2-1.

Segment 1, Ground Application Errors:

This is the service provider segment. Segment 1 errors include failure of the application from performing its functions, content errors or inaccuracy, and failures of the hardware systems such as workstations that support the application.

From a network management perspective this segment is outside the scope of this CONOPS. However, in the case where a failure in this segment affects neighboring segments, the detecting service provider needs to inform neighboring segments of the problem while taking immediate actions to isolate the problem. This may include discarding messages to prevent buffer overflow or circulation of erroneous messages in the network.

Segment 2, Data Network Errors:

Segment 2 refers to the ground ATN internet as well as to auxiliary subnetworks in the Day1 scenario defined in Section 1.1. Fault management of the data network at the element level, and some aspects at the network level, are practiced in the industry today. Most data network elements are equipped with management agents that automatically generate fault notifications to the managing system. Most failures in this segment can be detected by the management system and can be mitigated before affecting end-users. In addition, redundancy is typically designed into the network and that reduces user-affecting failures to a minimum. Failures may also be detected by neighboring domains. The reporting of failures across domains may be via trouble tickets between management systems. The neighboring domains may be a service provider, another network provider, an A/G network provider, or a leased line network provider.

Segment 3, Leased Line Network Errors:

Segment 3 errors are similar to segment 2 errors. In anticipation of failures, redundant lines are leased and configured to avoid single points of failure. Service is switched automatically to standby lines when a failure occurs.

Segment 4, A/G Network Errors:

In segment 4, a critical failure is the loss of A/G data connectivity. Because of limited bandwidth and airborne resources, redundant connectivity is handled differently from the ground/ground environment. There will generally be more than one air/ground subnetwork available and if there is not, in the near term, then voice backup will be available to provide an alternate means of communication. For example, VHF Data Link (VDL) MODE 2 has multiple frequencies, redundant Remote Ground Stations (RGSs), and/or alternate A/G network providers; while SATCOM DATA 3 has multiple satellites, alternate service providers and/or multiple connections. In addition, factors affecting the communication media (such as weather and atmospheric disturbance) are often beyond the control of the network provider and are difficult to predict.

Currently, A/G data connectivity may be assigned automatically by the network elements or manually by a network operator via a different communication means such as A/G voice.

A/G data transmissions often occur in random, short bursts. Keep-alive messages are employed in the network elements to reduce loss of connectivity. Loss of A/G data connectivity relies on end-user reports if there is not a mechanism in place for detection. A network management operator has little control or monitoring capability for A/G data connectivity unless provided by the network. However, network management operators are expected to monitor the network elements for other types of network failures to prevent connectivity loss from preventable causes.

Currently, manual mechanisms involving end-user initiation are employed. For quality and reliable A/G connectivity, the network should be designed to interconnect adjacent A/G data networks with trigger mechanism for automatic hand-offs.

In the near term, end-users may demand seamless connectivity from the A/G data network provider with penalties for connectivity failures stipulated in the bilateral service agreement.

The A/G data network providers will be expected to establish bilateral service agreements to share the responsibility for providing seamless connectivity. From a network management perspective it is difficult, if not impossible, to detect and prevent such loss of connectivity. Detection is typically by end-users thus sending notifications about the problem across domains may not serve much useful purpose for this case. This connectivity case is critical to the quality of A/G data communication. However, the key is in the network functions. Without seamless connectivity, there is minimal network management can do to overcome these loss of connectivity failures.

Segment 5, Airborne Network Errors:

Due to limited bandwidth & airborne resources, safety, and certification issues, real-time control and monitoring of airborne networks is to be avoided unless there is a safety-related need. A typical failure scenario could be as follows.

The airborne network element generates a short message to the aircrew signifying a failure. The crew then attempts to restore the network by re-setting the network element, if that capability is available. If this is unsuccessful, the network is shut down and the crew reports the problem to the ground via an alternative communication means such as A/G voice. Note that this message must reach the communicating parties and not the network management operators to establish alternative procedures. All network management notifications are logged on board for analysis when the aircraft is on the ground. Based on current understanding, it is not practical and perhaps unsafe to attempt to mitigate any fault in the airborne network from ground. Thus, there is no need for real-time monitoring of the airborne network from ground.

Segment 6, Airborne Application Errors:

Real-time management of the airborne applications is outside the scope of this CONOPS. Failures may be reported by the aircrew to initiate a switch over to alternate procedures. Note

again that this message must reach the ground communicating parties and not the network management operators in order to establish the alternate procedures.

Summary of the fault management processes:

1. To ensure ATN high availability and reliability, proactive maintenance is desirable.
2. The global span of ATN network coupled with participation by multiple organizations demands that faults be localized and isolated quickly. Each organization is expected to isolate and mitigate faults quickly and to prevent faults from spreading and affecting other areas.
3. Fault mitigation is to be handled without noticeably affecting other ATM services.
4. When source of a detected fault is outside an organization, the source organization needs to be notified in quickly so they can isolate and mitigate the problem.
5. Because of national security and reasons of air safety, direct interaction across organizations for network manager to agent operations is not advised
6. Due to limited bandwidth, management of communications over the A/G subnetworks is not done. Based on scenarios described previously, there is no identified need for real-time A/G network management exchanges.
7. ATN airborne equipment is expected to be maintained according to prevailing avionics standards and certification requirements. Real-time operational control of G/A avionics is not considered or expected.
8. The most direct and immediate way for detecting failures in an application process (for instance, CPDLC) is via detection of a time-out or the loss of connectivity in the network elements, or by means built-into the application processes. The display of detected failures immediately to the aircrew or controllers allows them to activate alternate procedures, such as switching to voice communication. The end system where the application process resides will also notify the network manager to activate fault mitigation procedures.
9. Each organization is expected to perform scheduled maintenance, with network element down time, in a manner that minimizes interference to the ATN network service quality. For example, the scheduled down-time for maintenance cannot introduce unpredictable traffic congestion nor increase message hops and delays in significant manner.
10. Each organization is expected to design its portion of the ATN network to avoid single points of failure.
11. When a scheduled outage is to affect ATM service availability, the initiating organization needs to notify the aviation community ahead of time via commonly acceptable means, such as the use of NOTAMs.
12. Remote testing and activation of diagnostic programs are desirable to enable timely verification of faults and to isolate faults before problems propagate throughout the ATN network.

13. To satisfy requirements for national security and for safety reasons, each organization is responsible and accountable for its network elements. Cross domain network manager to agent interaction is undesirable.
14. When a fault in one domain affects the quality of the neighboring ATN network, the fault must be isolated quickly and the affected neighbors notified immediately. For example, routing problems at a BIS or a faulty process in an end system that generate unacceptable or erroneous packets that will cause congestion in the neighboring ATN must be isolated and the affected neighbor must be notified to clear their buffers.
15. Cross organization communication of faults should be network manager to network manager via the standard means of trouble ticket information exchange.
16. The priority to be given to trouble tickets, based on the type of faults, can be agreed upon between organizations and standardized. Each organization is expected to take appropriate actions to resolve the trouble in an acceptable time. For example, high priority troubles should be handled immediately. This is to localize problems as quickly as possible and to reduce impacts on the quality of the overall ATN network.
17. In the case where failure of a router requires reconfiguration within each organization, it is expected that configuration information will be readily available to recover from the failure without delay
18. To achieve proactive maintenance, performance data and analyses of the ATN network need to be available on a regular basis and for actions to be taken to prevent failures. Each organization is expected to support performance analysis and recommendations for its own maintenance.
19. Each organization is expected to provide ATN network fault or down time information to its accounting process if such interruptions have affected services and or is required by the billing policy.
20. Each organization is expected to log events, alarms, and trouble ticket reports for a minimum duration. To ensure a minimum level of quality, organization may be audited for compliance in handling faults.

2.2.2.3 Performance Management Process

The general performance management process is illustrated in Figure 2-8. Each organization is responsible for collecting and storing performance information from its own portion of the network. Most data network elements are capable of providing performance data to a network management system on a scheduled basis. Typically, performance data is collected and stored for future analysis and is not handled in real-time. Thresholds may be preset such that, when performance is degraded beyond a threshold for a given time, the network element reports the situation as an alarm notification of a high severity. The notification is then handled in real-time by the fault management process. The mechanisms for

setting up the thresholds, schedules, and selecting relevant performance data for collection are employed in commercial data network elements.

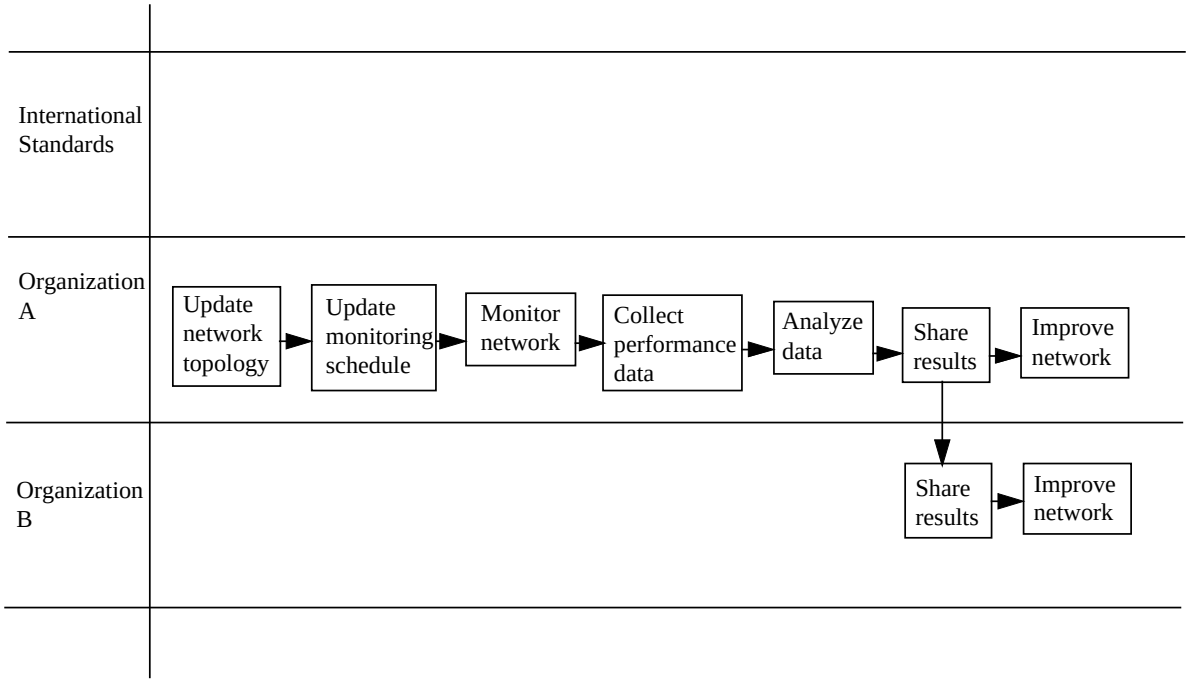

Figure 2-8 Performance Management Process

The set of performance data defined for collection in an organization depends on the operational purpose and the usage of the data. For example, traffic counts are collected for network expansion planning. Packet loss counts and packet error counts may be used to determine network performance degradation. Various error parameter counts from the communication layers are used for detecting communication layer degradation as well as connectivity performance. Some performance data may also be used for billing. In that case, relevant performance data are forwarded to the accounting process.

There are advantages to sharing performance data and analysis results across management domains. These include:

1. Availability of performance data for billing purposes
2. Detection of network degradation due to adverse effects from interconnected elements
3. Improvements in network performance from re-configuring interconnected elements based on shared data
4. Awareness of performance degradation detected from outside of the management domain

In the bilateral service agreement between two organizations, based on the level of collaboration and billing methods, specific performance data and analysis results are selected for exchange on a regular basis. In addition, the ATN community may recommend certain levels of performance collaboration to ensure ATN quality. Typically in the industry, performance analysis is done on an ad hoc basis within an organization and without any specific industry standards.

Regular performance analysis of the ATN network is a simple method to achieve proactive maintenance. By understanding the ATN network performance patterns under normal operation, degradation can be quickly identified from any performance anomalies.

Consider the case where bad weather is expected in a region: A/G communications via the ATN may substantially increase in that region for weather updates and re-route requests and approvals. If the ATN capacity and traffic trend is known for normal conditions, procedures for handling a sudden traffic load increase can be derived. For example, if sufficient prediction is available and additional resources are available, re-configuration or re-routing of network traffic to handle the increase load can be executed. Alternatively, the use of A/G subnetworks could be canceled by relying solely on voice broadcasts in the affected region.

Summary of the performance management process:

1. Common, standardized performance data is expected to be readily available from the ATN network elements.
2. Performance analysis is a cost effective way to achieve proactive maintenance for ATN networks.
3. Each organization is expected to analyze the ATN network performance data on a regular basis. They are expected to take appropriate action to mitigate degradation and to ensure ATN service quality.
4. Each organization is to inform adjacent organization of a ATN network performance degradation that affects that organization. The potential problem, the planned actions, and the time frame for mitigation are shared across organizations. Similarly, ATN performance degradation detected by adjacent organizations is expected to be communicated to the source organization.
5. If a change in ATN network traffic patterns across organizational boundaries is expected, the affected organizations need to be informed.
6. There is no identified need to exchange raw ATN performance data across organizational boundaries on a regular basis. Cross organization manager to agent communication is not necessary and is not advised. If the sharing of raw data is agreed upon between organizations, only data pertaining to those organizations should be shared and not third party data. For example, if raw ATN traffic data is to be exchanged between two organizations, the collected traffic data needs to be processed to eliminate traffic

information concerning other organizations. This is to protect and honor organizational privacy and to avoid national security implications.

7. Selective sharing of performance analysis results across organizations based on agreement could help in establishing effective maintenance coordination.
8. Each organization is expected to forward performance data to the accounting process if the data is required.
9. Each organization is expected to provide performance analysis results and recommendations to its configuration management process to refine or improve ATN network performance. Impacts on the overall regional ATN network must be considered.

2.2.2.4 Accounting Management Process

The accounting management process is likely to vary among organizations based on billing practices. For example, customers may be billed for usage, connections, packet counts, a combination of these, or other means. Network management is responsible for collecting the pertinent raw data and then forwarding the data to a finance department to be processed for each customer. Some data processing may be performed before forwarding to the finance department. This may take into account refunds due to network errors or congestion beyond the acceptable level stated in a bilateral agreement.

Figure 2-9 illustrates a general accounting management process. Generating bills and collecting bills are typically outside the network management functions. Organizations may agree to exchange raw usage counts for verification of the data. However, this is not typically done currently in the industry. Upon occasion, requests for verification of bills arise. This is typically handled through the finance process rather than the network management process.

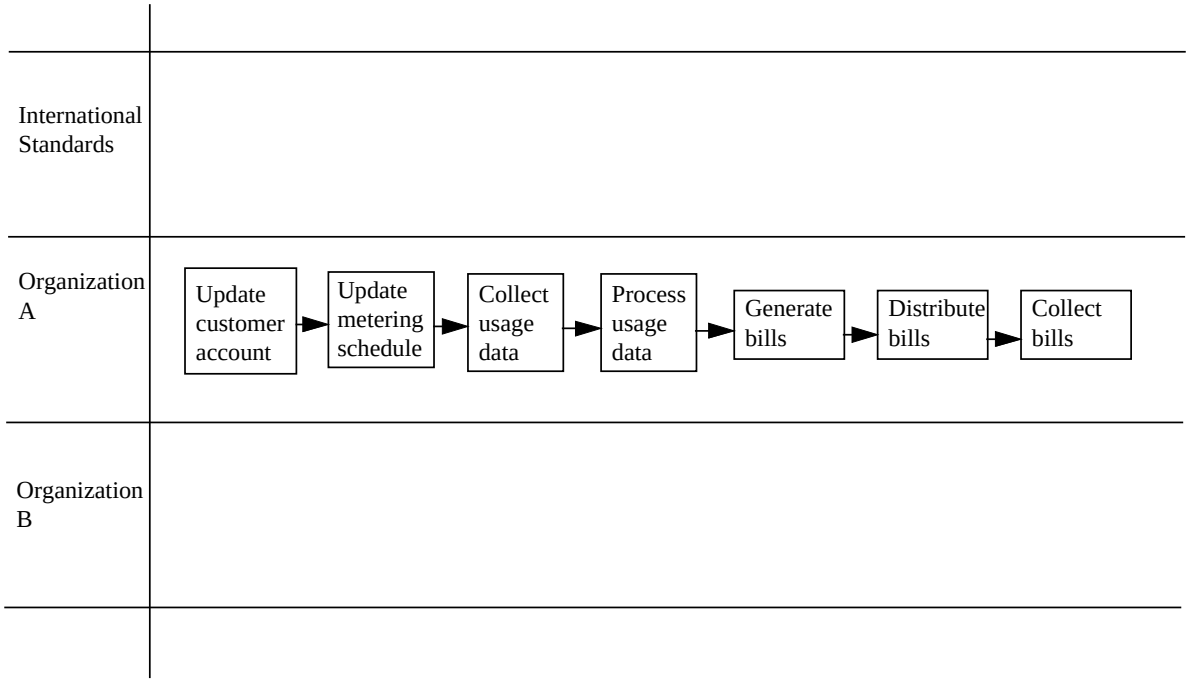

Figure 2-9 Accounting Management Process

Usage data exchanged between two organizations in a network management process may come about when there is agreement to provide the data for performance analysis. However, it is more likely that the data is routed to the performance management process for analysis before exchanging it between organizations.

Due to the sensitivity of the data for accounting, exchange of raw data at this level is kept to a minimum and typically non-real time.

Summary of accounting management interaction across organizations:

1. Inter-exchange of accounting data is based on a bilateral agreement between two organizations.
2. Exchange of raw usage counts is not necessary unless agreed upon by the organizations.
3. There is no identified need for real-time exchange of data for ATN network accounting management.
4. There is no identified requirement for cross organizational manager to agent collection of accounting information.
5. If the exchange of raw data becomes necessary across organizations, data regarding other organizations must be extracted before forwarding.
6. Accounting typically involves additional processing besides the collection of metering data, thus raw data sharing at the boundary is not always reflected in the bills.

7. Data collected for accounting may be used for other purposes such as for performance analysis. In these cases, the data should be processed to protect an organization's privacy and security and forwarded to the appropriate processes for analysis. Each organization is expected to protect information pertaining to other organizations on a need to know basis.
8. Refer to the contribution to ICAO on accounting scenarios for details.

2.2.2.5 Security Management Process

This section describes the key issues, decisions, and concerns when planning the security management aspects within and across individual management domains. Technical processes for Day1 ATN network security management operations are not discussed, but will be included in future updates as the requirements and SARPs are developed by the ICAO technical committees that are actively pursuing these topics.

The general issue of ATN security is deferred to the appropriate ICAO documents for a complete discussion.

Most security management processes are confined to addressing the control of access to system resources through physical security procedures, authentication techniques, and access authorization policies. However, there are two additional aspects of security that deserve fuller consideration. The first is the management of security processes for the network as a whole. This involves distribution of keys, updates of authentication codes and authorization lists, and notices of system penetration or of 'rogue' devices.

The second aspect of security for network management is the protection and security of the network management processes themselves. If the network management system becomes compromised, it can have grave consequences for the health and security of the network generally. Also, the network management processes may be conveying information that is confidential or proprietary to a particular management domain.

As a minimum, the network management process requires the following security services to secure its own operations:

- Physical security of network devices and resources
- Authentication of sources and other anti-spoofing techniques
- Protection from corruption for network management data and messages
- Security against unauthorized disclosure of data

Section 3

Roles of ATN Organizations

This section describes the organizations that will participate in the ATN network. It defines their roles and their responsibilities for managing the ATN network in the context of the environment previously described in Section 2. The interactions and inter-relations between management domains and organizations are addressed.

3.1 ATN Roles and Responsibilities

The ATN participants are described according to the model shown in Figure 3-1. This provides a framework for discussing their roles, responsibilities and functions in the ATN. These basic units serve as building blocks to describe the roles and responsibilities of complex organizations such as the airlines and CAAs in the evolving environment.

3.1.1 End-Users

This group of participants uses the services available through the ATN network for their operational needs. For example, pilots, airline dispatchers and ATC controllers are users of AOC services as well as of CAA services.

3.1.2 ATN Data Service Provider (ADSP)

An ADSP provides the end services to the end-users. They own and maintain the applications or services that are delivered via the ATN network, and they can also be end users. For example, a Civil Aviation Authority (CAA) is considered an ADSP for the delivery of flight clearances, for maintenance of separation, or for the conduct of other ATC activities. In this case, the Air Traffic Service Provider (ATSP) is an ADSP. ADSP also includes those who provide value-added aviation services such as weather information or digital ATIS. However, the service provided by a CAA will most certainly be safety-critical and not on the same footing as the more usual data services available from other ADSPs.

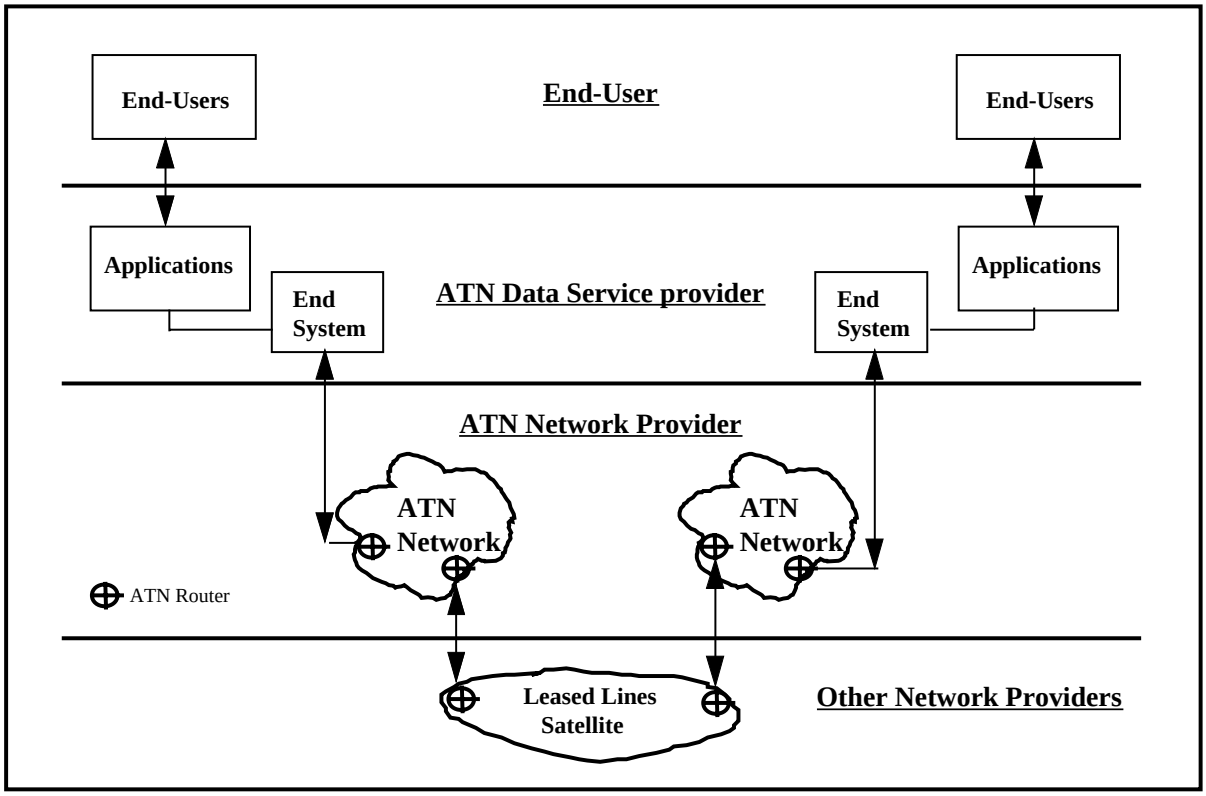

Figure 3-1 Model of ATN Participant Relationships

3.1.3 ATN Network Provider (ANP)

An ANP owns or controls portions of the network elements that make up the ATN network. An ANP provides a backbone ATN network that interconnects end users and ADSPs for the purpose of obtaining or distributing services. Any organization such as Aeronautical Radio, Inc. **(**ARINC) or the Societe Internationale de Telecommunication Aeronautiques (SITA) owning or controlling ATN routers is an example of an ATN network provider.

ANPs must provide a network architecture that will support a distributed communication topology in a manner similar to that provided by current G/G aviation communication service providers. The network architecture must be flexible and adaptable enough to support the expected growth in type and volume of aviation message traffic. The network should support a variety of A/G subnetworks, including HF, VHF, satellite, or any future ICAO standard subnetworks. The network should support all ATN procedures to permit routing to any aircraft on a worldwide basis.

The ANP should be capable of providing support within their domains to legacy

communications systems until the evolution to a fully deployed ATN infrastructure is achieved.

ANPs will use network management processes to assure service quality, that is, end-to-end system performance, security controls, message integrity, available system capacity, and message delay within their domains. The same procedures would be applied to adjacent domains operating under an SLA.

ADSPs will require that ANPs be capable of concurrently handling both ATC and AOC traffic and provide the ICAO standards for priority and routing policy applicable to each class of traffic. ADSPs also envision a future need for network services that will be able to handle digitized voice messages as well as standard data communications.

Because they are expected to normally operate in a multi-user environment where they are interconnected with many administrative and management domains, the ANP will have to deal with many test and certification issues. Before entering an SLA with any entity, the ANP will rely upon direct or third-party testing and certification of technical interfaces and access protocols. Operationally, the ANP should support network mechanisms to dynamically provide authentication of users and message sources and to assure that offered message traffic will be routed to known, valid destinations.

3.1.4 Other Network Providers

This group of participants consists of network service providers that are not connected directly to ATN data service providers. For example, satellite communication provider and leased-line communication provider are indirect ATN network providers. These other (indirect) networks, can have effects on the overall ATN service quality. The management of data link communication connectivity needs to be seamless and transparent to the end-users.

3.2 ATN Organizations

This section describes the organizations participating in the implementation, management and use of the global ATN network.

3.2.1 Commercial Airlines

Commercial airlines, as versus GA or the military, own and control both their ground infrastructure and their airborne assets within a commercial airline administrative domain. For example, commercial airlines, through IATA, are responsible for the assignment and maintenance of Transport Service Access Point (TSAP) and NSAP addresses for all airborne routers and end systems, including those used for ATM with state systems on the ground. IATA airlines are the same as any State when it comes to sharing managed objects (MOs) across administrative boundaries, network agent-to-manager or manager-to-manager. In

general, IATA airlines do not intend to open either their airborne or their ground based networks to other airlines, international network service providers or States. However, IATA airlines are ready to negotiate with States on a common, agreed-to minimum set of MOs that all users of the ATN agree to share with all other users of the ATN, both agent-manager and manager-manager. For the sharing of MOs over A/G links, IATA airlines expect that the ground based requesters may be charged a fee for usage that exceeds prior agreements. IATA airlines envision one airborne agent co-resident with their one airborne BIS for Day1 operations. IATA airlines intend to provide for the dynamic uplink and downlink of some system management information to and from the airline ground based managers, but they reserve the right to decide whether or not to do dynamic uplinks and downlinks on a flight-by-flight basis. IATA airlines also expect that some system management information will be stored onboard for retrieval via less costly ground-ground circuitry after landing. IATA airlines, finally, expect that not all IATA airlines will implement system management as described above. Some airlines are likely to rely on their preferred international ATN network service provider for system management support. This is viewed as a general option to out source system management responsibilities to trusted third parties, who then become part of an IATA airlines management domain (that is, a management domain that crosses administrative boundaries).

Typically, a commercial airline takes on a combination of the basic roles. The airline is an end-user (pilots and dispatchers), an ADSP (providing AOC type services to its end-users), and an ANP (with its own ATN routers in its control centers and selected airports/hubs).

3.2.2 Aeronautical Communication Service Providers (ACSP)

An organization in this category owns and controls their own G/G and A/G communications infrastructure. Access to the communication services built on this infrastructure is offered to all other organizations in the aviation community. They have well developed accounting management systems to support billing for services rendered. ARINC and SITA are the principal examples of this type of organization.

The aeronautical service provider organizations also offer end-to-end value-added applications services over their network infrastructure to commercial airlines and to CAAs. They also typically operate legacy communication services that must be transitioned to the ATN network

They may enter into communication service agreements with equivalent service provider organizations in order to mutually offer services over a wide domain.

An ACSP is likely to take on the combine roles of being an ADSP providing aviation services such as weather information, and an ANP for its own ATN routers network before interconnecting to a backbone ANP.

3.2.3 Civil Aviation Authorities

CAAs own or control their own ground infrastructure. CAAs are responsible for the assignment and maintenance of the NSAP addresses for each ground system, and for the assignment of TSAP addresses to applications running on a particular system. When providing services to GA, CAAs may also provide address assignment facilities. CAAs are responsible for the operation and management of all assets within their administrative domain.

In some instances, CAAs may choose to contract for some ATN services. In this case, the contractor will act in the capacity of a CAA and will be assigned addresses and be managed as part of the CAA's management domain.

In other instances, CAAs may choose to form collaborative arrangements with other CAAs for the purpose of administration and management. In this case, each CAA maintains its own administrative domain and management domain even if one entity provides the service for other entities.

Typically, a CAA takes on a combination of the basic roles. The CAA is an end-user (ATC controllers), an ADSP (providing ATM services such as CPDLC), and an ANP (with its own ATN routers in the various control centers before interconnecting to a backbone ANP).

3.2.4 General Aviation

The GA community encompasses a wide range of aviation activities, from single-engine, single-pilot aircraft to high-performance aircraft with professional aircrews. The high-end GA operators will use the ATN on nearly the same basis as will the commercial airlines. They may contract with commercial airlines or ADSPs for specific services.

GA is unlikely to be participating in Day1 operation and will not be elaborated in this version of the CONOPS.

3.2.5 Military Users

Military users are presumed to operate in a manner that combines features of the operations of commercial airlines and of the CAAs. Military users need CNS/ATM to facilitate their operation of regional and global logistical activities in support of their military mission. Because of this they will use ATN networks and end-to-end services.

Where the ATN services are available, military users are expected to participate in the ATN as do commercial airlines, and taking into account their agreements with the appropriate CAA authorities to utilize the airspace.

In those cases where military users need to conduct operations in restricted airspace, or where ATN service is not available, they will provide their own ATN services including G/G and A/G infrastructure. In this case, the military will maintain it's own administrative and

management domains. These domains will interoperate with the global ATN seamlessly. These services will not be available to commercial organizations.

Where the military users have special security needs (such as for transmitting air-tasking orders) which are not provided for in the ATN, they will operate their own end-to-end security applications over the ATN. Such applications will not be used or managed by any other organizations.

3.3 Fully Operational ATN Environment

The following describes a fully operational ATN environment (i.e., global steady state of the ATN). This high level description serves as a reference for discussion of ATN network management on Day1 of ATN operation.

Figure 3-1 illustrates the global ATN network composed of a series of ANPs connecting CAAs, Airlines, and ACSPs that are linked both technically by ATN routers and administratively by SLAs. CAA 1, as an example, has an agreement with ANP 1 for end-to-end ATN connectivity to CAA 2, or perhaps ACSP 2. ANP 1 provides ATN service by arrangements with local providers A, B, and C. ANP 1 also has an agreement with ANP 2 for ATN network service connectivity outside the area in its control (for example, traffic destined for Airline 2).

End-to-end connectivity between, for example, Airline 1 and CAA 2, is achieved through a similar pattern of interconnection agreements.

This global steady-state of the ATN environment is desirable because it allows the CAAs and airlines to focus on their key operational responsibilities of providing air safety through ATM services and safe air transport. This environment also allows network providers to be flexible in expansion of the ATN network by forming alliances or evolving its own ATN network segments and A/G communication infrastructure. The environment simplifies SLAs for all organizations in that they can quickly join the ATN network by signing an SLA with a network provider. This environment encourages innovation in providing aviation services.

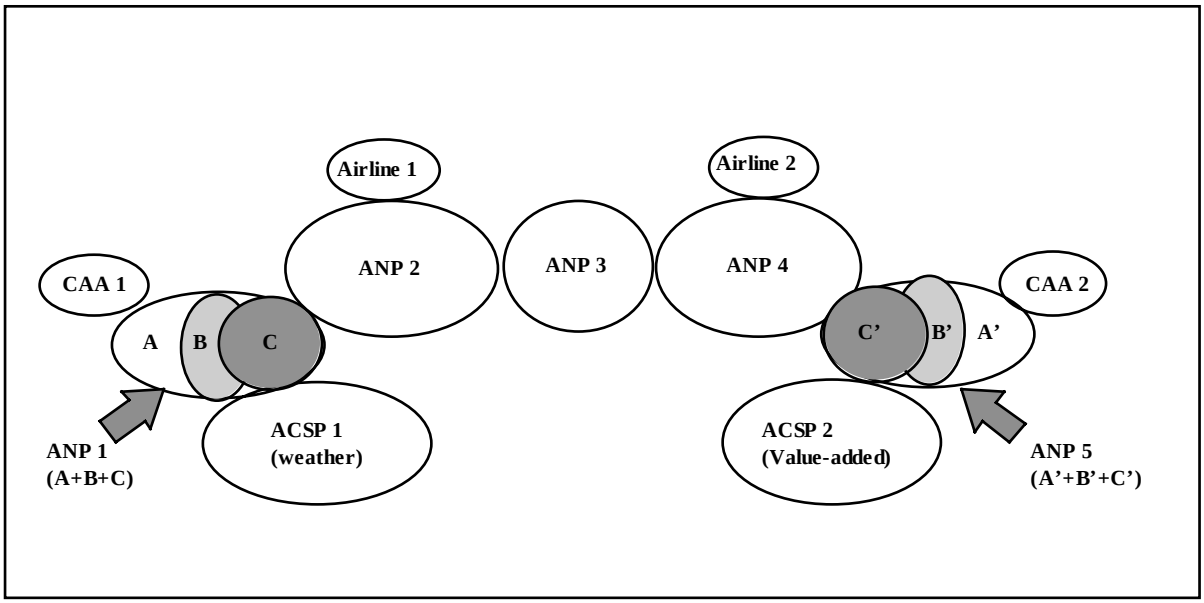

Figure 3-2 The Global ATN Network

The global steady-state environment represents a common goal for the ATN community. Airlines and CAAs are expected to encourage network providers to form alliances in building an ATN and A/G communication infrastructure.

In the near term, ATN trials are likely to be regional. An example is the transpacific ATN trial between the CAAs of Japan and the US. Both CAAs will be responsible for the network and the services, as well as acting as the end users of the ATM ground applications.

To illustrate how the long term concept works, the following subsections describe scenarios from CAA and Airline perspectives.

3.3.1 CAA Perspective

When selecting its ATN network provider a CAA has two major needs:

1. To communicate with all its ATC sites and with all other CAAs globally via the ATN network.
2. To provide ATM applications to all aircraft in the Flight Information Region (FIR) it serves.

The consequence of the first need for the CAA is that it must ensure that the ground ATM applications are running accurately, are available at specified times, and are maintained regularly. The CAA is responsible for providing the G/G ATM services.

Another consequence of the first need for the network provider is that it must ensure

delivery of the ground ATM application data to and from the CAA's sites and other CAAs. The network provider can achieve this either by using its own networks entirely or, more likely, by forming alliances and connectivity with other network providers. The network provider is responsible for end-end connectivity. The first provider holds other network providers responsible for their portions of the ATN connectivity.

The consequence of the second need for the CAA is that it must ensure that its airborne ATM applications also are running correctly, are available at specified times, and are maintained regularly. The CAA is responsible for providing the G/A ATM services.

Another consequence of the second need for the network provider is that it must ensure delivery of the air ATM application data to and from the CAA's ATC sites and aircraft in the region. The network provider can achieve this either through its ground ATN network to its A/G communication network in the region or by forming alliances with other network providers, including satellite communication providers, to provide A/G connectivity. The network provider is responsible for A/G and G/G connectivity and holds other network providers responsible for the portions that are under their control. This includes providing mechanisms for A/G subnetwork to A/G subnetwork hand-off.

3.3.2 Airline Perspective

Similarly, when selecting its ATN network provider an airline has two major needs:

1. The airline wants to communicate among all its Airline Communication Centers (ACC) and with CAAs globally via the ATN network.
2. The airline wants its aircraft to be in data communication with its ACCs and with CAAs when airborne.

The consequences are similar to the CAA-network provider scenario. The airline is responsible for ensuring the operation if its air and ground AOC/ATM applications to all the CAAs. Again, the network provider is responsible for end-end connectivity and can achieve it via different means, including forming alliances with other network providers and holding them responsible for their portions of the ATN network.

3.4 Global Partnership

This section is reserved for addressing network management issues that cannot be adequately covered by pairwise agreements (SLAs) between organizations. Issues such as global disaster recovery plans and primary route selections are potential examples. Further analysis and inputs are required to determine the issues in this category.

Section 4

ATN Management Functions

This section examines the network management functions relevant to the ATN. The purpose is to establish a minimum level for all organizations to sustain the network and to support the ATN environment described in Section 3. The management functions are presented in two subsections: the expected management functions for an administrative domain and the expected management functions for cross-administrative domains.

Network management in this context includes all layers of the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Telecommunications Management Network (TMN) standards from the business management layer to the element management layer. Business management concerns (such as the degree of partnership, coordination, responsibilities, management data, and profit sharing) are briefly discussed only in the context for establishing integrated management in the global environment. Similarly, for service management, Service Level Agreements (SLA) between organizations are discussed in the context of establishing global service quality uniformity.

The operations functions necessary to maintain network quality of service are discussed at a high level from a CONOPS point of view. These functions, as well as the detailed requirements, serve as a check list for drafting bilateral SLAs. More stringent agreements could apply based on negotiations between organizations. Depending on the scale of the ATN network, some functions may need to be expanded and become more elaborate or they may be reduced. For “Day1” control of the ATN network elements, section 4.1.3 outlines the basic daily management functions and expectations.

4.1 General Responsibilities for an Administrative Domain

This section covers the responsibilities expected in each administrative domain. The assumptions are that:

1. Each administrative domain will ensure that its portion of the ATN is designed without any single points of failure.
2. Each administrative domain is to ensure that all indirect network elements (non ATN, see 3.1.4) connected to its portion of the ATN will not cause network degradation.
3. Each administrative domain is to have full control of its portion of the ATN network. Administrators must maintain and provide archives of management for quality auditing.

4.1.1 Operation Planning

This section provides guidance for each administrative domain on operation planning functions for its portion of the ATN network. Operation planning is the work performed in preparation for activation the ATN network or addition of ATN network elements for daily use. Several plans need to be in place before actual operation of the ATN. For future expansion the plans are also reevaluated based on experience from actual operations. These plans are important in assuring that an ATN network segment operates at the required service quality. A check list of operational plans and expectations for the ATN community is provided below.

4.1.1.1 Planning for evolution and expansion.

1. Each administrative domain is expected to ensure that there are no single points of failure within its ATN network.
2. Each administrative domain is expected to ensure that its portion of the ATN is not a source of regional failure in the case of a catastrophic failure of its ATN network.
3. Each administrative domain is expected to ensure that its portion of the ATN network can continue to provide services when interconnection to neighboring domains must be disconnected (for instance, in the case of isolation from a major fault).
4. Each administrative domain is expected to ensure that local priorities and expansion of services do not remove resources from ATM services or compromise air safety.
5. Each administrative domain is expected to ensure equipment compatibility when introducing new routers.
6. Each administrative domain is expected to ensure minimum impacts to existing ATM services during expansion.
7. Each administrative domain is expected to maintain complete control and maintenance of its portion of the ATN during and after completion of expansion.

4.1.1.2 Disaster recovery planning and procedures development.

In the event of catastrophic failures due to, for instance, an earthquake, each administrative domain is expected to have a detailed disaster recovery plan and procedures for its portion of the ATN network. The plan is to be kept current by periodic reviews and drills on the procedures.

4.1.1.3 Management systems compatibility for sharing information.

For sharing management information electronically from network manager to network manager, each administrative domain is expected to implement a standards-based approach. The specific information being exchanged may be beyond the standards requirements based on SLAs. This is to eliminate the costs of implementing multiple proprietary solutions when

exchanging data with more than one organization.

4.1.1.4 Methods for interaction.

1. Each administrative domain is expected to establish internal management processes to coordinate management functions to support its portion of the ATN. For example, a process for coordinating access to configuration information to mitigate a fault or forwarding performance and fault records to accounting, needs to be in place.
2. Each administrative domain is expected to establish the means for external interactions for coordinating ATN management functions across organizations. Examples are: points of contact, escalation procedures when needed, manager to manager exchange of management information.

4.1.1.5 Security planning.

Each administrative domain is expected to have a security management plan.

4.1.1.6 Interconnection agreement negotiating and planning.

1. Each administrative domain is expected to ensure systems interoperability when connected with other organizations. This includes network manager to network manager and network element connectivity. The connection must not affect the performance of the ATN network nor of the manager systems.
2. Each administrative domain is expected to ensure that additions to the ATN network do not affect operation of the existing network before becoming operational.

4.1.1.7 Overall workforce planning.

1. Each administrative domain is expected to ensure workforce coordination so that pertinent ATN information is kept up-to-date and available to the appropriate personnel. For example, configuration information and NSAP addresses for new network routers needs to be provided by the network engineers to the network management operators.
2. Each administrative domain is expected to schedule and assign management tasks so that ATN problems are isolated and resolved quickly.
3. Each administrative domain is expected to designate points of contact for daily management functions across administrative domains. For example, if a cross organization trouble ticket is not handled within a certain time, the adjacent organization needs a point of contact for an inquiry.

4.1.1.8 Management procedure development.

Each administrative domain is expected to have management processes and procedures in place to ensure the health of the ATN network. This includes handling of cross organization

management requests, trouble tickets, and for escalation of management and network design decisions such as major configuration or performance changes.

4.1.1.9 System integration planning.

1. Each administrative domain is expected to ensure that all equipment is certified and operationally approved before connection to the global ATN network. This includes management systems as well as cross organization equipment and systems.
2. Each administrative domain is expected to perform appropriate integration tests of all equipment before introducing into the ATN network.
3. Each administrative domain is expected to keep new ATN network equipment under special control and observation for a period of time to ensure proper integration. Criteria for evaluating integration success should be provided to the network management operators.
4. Each administrative domain is expected to be able to immediately isolate newly installed equipment in their domain in case there are failures during integration period.
5. Each administrative domain is expected to coordinate integration efforts between its network engineers and network management operators to ensure seamless transition from the integration phase to complete operation.

4.1.2 Operations Engineering and Analysis

This section addresses functions performed after installation of network equipment and the ATN is under supervised operation. These functions can also be viewed as second tier functions in support of tier 1 management functions (section 4.1.3). The check list and expectations of the ATN community are provided below.

4.1.2.1 Reliability of management information.

1. Each administrative domain is expected to ensure that its network manager software is receiving, and is capable of providing, accurate and correct management information to and from the ATN network element agents.
2. Each administrative domain is expected to ensure that management information is exchanged between its network manager and agents without delay.
3. Each administrative domain is expected to ensure accuracy and correctness of ATN management information before forwarding to other organizations
4. Each administrative domain is expected to only exchange previously agreed management information.
5. Each administrative domain is expected to remove sensitive ATN management data from the information before forwarding it other organizations in order to protect organizational

privacy and confidentiality.

6. Each administrative domain is expected to only exchange ATN management information pertaining to each organization with whom it has an agreement and to not forward third-party management information.

4.1.2.2 Path for management information in ensuring availability.

Each administrative domain is expected to ensure management connectivity to its ATN network for 24x7 monitoring and control.

4.1.2.3 Capability to manage the network within the administrative domain.

Each administrative domain is expected to provide management capabilities to its ATN network. For example, each domain needs to ensure timely dissemination of configuration information to its own ATN network, to perform alarm correlation and isolate faults, to analyze ATN performance, and to collect usage metering for accounting.

4.1.2.4 Performance analysis.

1. Each administrative domain is expected to analyze performance data on a regular basis. Key performance data includes packet loss counts, packet error counts, and connection re-establishment counts.
2. Each administrative domain is expected to establish the normal operational pattern of its ATN network based on performance analysis. When appropriate, recommendations to refine its ATN network configuration for better performance is desired.

4.1.2.5 Traffic analysis and planning.

1. Each administrative domain is expected to analyze traffic data for its ATN network on a regular basis. Based on the analysis, the normal traffic patterns are established as a basis for evaluating the domain's ATN network capacity. This allows network engineers and network management operators to be more responsive to changes in traffic patterns or in traffic loads.
2. Each administrative domain is expected to monitor traffic priorities to ensure that ATN resources are adequate and are allocated properly.

4.1.2.6 Conformance / interoperability testing.

Each administrative domain is expected to ensure that ATN network elements are interoperable and conform to ATN network standards and perform at an acceptable quality. This also includes interoperability and conformance for network management systems. The actual conformance and interoperability tests may be performed by an authorized organization.

4.1.2.7 Management system update, installation, and deployment.

TBD

4.1.3 Service and System Management

This section addresses the five functional areas of configuration, fault, performance, accounting, and security. These functions are performed by network management operators on a full-time basis. It is the main bulk of managing the ATN. These can be considered tier 1 functions (see 2.2.1).

4.1.3.1 Security of subnetworks.

TBD

4.1.3.2 Handling of configuration changes that impact other administrative domains, including interference.

1. Each administrative domain is expected to ensure the accuracy of the network management information. For example, configuration information for ATN routers must be verified to be complete and correct before distributing it to the ATN routers.
2. Configuration changes are likely to affect more than one router. To avoid long down times for upgrading the configuration and for reducing errors in propagating the changes, automation within a domain is desirable.
3. Configuration responsibilities are often shared between network engineers and network management operators. Within a domain, it is expected that coordination between the different functional groups will be encouraged to ensure the continued ATN network operability.
4. Every organization is expected to backup configuration information and to keep it at a physically separate location. Each organization must have a disaster recovery plan in case of catastrophic failures. The recovery plan needs to be understood by all responsible personnel. This includes periodic drills to familiarize and prepare personnel to handle the disaster situations.

4.1.3.3 Logging of management information.

Each organization is expected to log events, alarms, and trouble ticket reports for a minimum duration. To ensure a minimum level of quality, organization may be audited for compliance in handling faults.

4.1.3.4 Fault management, trouble administration.

1. In the case where failure of a router requires reconfiguration within each organization, it is

expected that configuration information will be readily available to recover from the failure without delay.

2. To achieve proactive maintenance, performance data and analyses of the ATN network need to be available on a regular basis and for actions to be taken to prevent failures. Each organization is expected to support performance analysis and recommendations for its own maintenance.
3. Each organization is expected to provide ATN network fault or down time information to its accounting process if such interruptions have affected services and or is required by the billing policy.
4. Remote testing and activation of diagnostic programs are desirable to enable timely verification of faults and to isolate faults before problems propagate throughout the ATN network.
5. To satisfy requirements for national security and for safety reasons, each organization is responsible and accountable for its network elements. Cross domain network manager to agent interaction is undesirable.
6. Each organization is expected to perform scheduled maintenance, with network element down time, in a manner that minimizes interference to the ATN network service quality. For example, the scheduled down-time for maintenance cannot introduce unpredictable traffic congestion nor increase message hops and delays in significant manner.
7. To ensure ATN high availability and reliability, proactive maintenance is desirable.
8. The global span of ATN network coupled with participation by multiple organizations demands that faults be localized and isolated quickly. Each organization is expected to isolate and mitigate faults quickly and to prevent faults from spreading and affecting other areas.
9. Fault mitigation is to be handled without noticeably affecting other ATM services.

4.1.3.5 Performance management, degradation.

1. Each organization is expected to forward performance data to the accounting process if the data is required.
2. Each organization is expected to provide performance analysis results and recommendations to its configuration management process to refine or improve ATN network performance. Impacts on the overall regional ATN network must be considered.
3. Each organization is expected to analyze the ATN network performance data on a regular basis. They are expected to take appropriate action to mitigate degradation and to ensure ATN service quality.

4.1.3.6 Data/information resource management.

1. Each organization is expected to maintain its configuration information with copies stored

at physically separated locations.

2. Each organization is expected to schedule for periodic update of configuration backup information on separate storage media.
3. Each organization is expected to maintain a copy of its configuration information that can be used to revive their portion of the ATN network in case of catastrophic failure of the network.
4. Each organization is expected to protect data and information pertaining to other organizations and honor privacy.

4.1.3.7 Service negotiation.

TBD

4.1.4 Supporting Management Functions

This section briefly addresses other management functions that each administrative domain should be aware of, but the functions do not directly impact the overall service quality of ATN. Discussion included are:

- Inventory.
- Human resource management.
- Customer network management.
- Interface with customers plans and procedures.
- Trouble reports and customer relations.
- Help desk operation.
- Network QoS maintenance costs.

4.2 Management Functions for Cross-Administrative Domains

This section provides guidelines on management functions for cross-administrative domains in support of the interconnection SLAs between ATN participants. It focuses on major management functions that impact overall service quality.

The functions are discussed at a high level from a conceptual view point. Detailed management functional requirements are left for a separate document. These functions, as well as the detailed requirements, serve as a check list. More stringent functions may apply based on negotiation between the organizations. Depending on the scale of the ATN, some functions will need to be expanded and become more elaborate or will be reduced in the level of involvement.

4.2.1 Business Partnership

This section addresses business management functions between administrative domains in support of an SLA. It establishes the basis for the types of service and network management information and services to be exchanged across administrative domains.

4.2.1.1 Clear identification of partnering relations.

In a bilateral service agreement, the organizations involved state clearly their roles, responsibilities, and expectations for each other. For example, an organization needs to state whether it is a network provider, service provider, end user, or a combination of these. As a minimum, a network provider is responsible for seamless connectivity; a service provider is responsible for ATM, AOC, or other aviation related services; and the end user is responsible for application compatibility and proper usage of the applications.

4.2.1.2 Contact personnel for timely coordination in restoring a network.

Cooperating organizations need to provide each other with management contact information. This includes contacts for these activities:

1. handling daily management operation exchanges, such as query for past due trouble tickets, clarification of configuration change requests,
2. executing joint disaster recovery plans for catastrophic failures,
3. contacting supplier field engineers, in the case where a network failure requires supplier expertise to restore the network.

4.2.1.3 Coordination planning.

Organizations should agree on their coordination processes and procedures. This includes handling trouble tickets, configuration change requests, responding to performance analysis results, disaster recovery, and other agreed management coordination issues.

4.2.1.4 Data management.

[Priority data, message polling frequency, usage of data for management or for use by other administrative domains, ownership and payment issues.]

1. Each organization is expected to protect data and information pertaining to other organizations and respect organization privacy.
2. Each organizations is expected to only share data and information of the agreed organizations.
3. Each organization is expected not to share information or data of other organization without the consent of those organizations.

4.2.1.5 Management of airborne equipment.

TBD

4.2.1.6 Configuration changes and certification issues.

TBD

4.2.1.7 Disaster coordination.

TBD

4.2.2 Interconnection Agreement for End-to-End Service Provisioning

This section addresses service management functions between administrative domains in support of an interconnection agreement. Functions may include: [TBD, need more research]

- Responsibility of end-to-end service integrity—how to monitor and ensure reliability, redundancy, auto switching to backups, who is responsible.
- Service availability and criticality.
- Service reliability.
- Service quality measurements.
- Interconnectivity—system and network integrity, interference testing.
- Extent of connectivity monitoring/management, responsibility, hand overs, path integrity, and notifications.
- Required Communication Performance (RCP).
- Installed Communication Performance (ICP).
- Actual Communication Performance (ACP).

4.2.3 Network and System Coordination

This section addresses the network and system management functions between administrative domains in support of an interconnection agreement. Functions may include:

4.2.3.1 Interface compatibility.

TBD

4.2.3.2 Shared performance and status data

Specific issues for each of the five functional areas: configuration, fault, performance, accounting, security. TBD

4.2.3.3 Shared information.

How often, immediate notifications for types of failures, what information to share, how to process the information, notification of disaster or emergency failures, etc. TBD.

4.2.3.4 Mode of sharing information.

TBD

4.2.3.5 Electronic, procedures, security.

TBD.

4.2.3.6 Responsibility for accuracy of information.

For example, how to handle outdated information in queue or delayed due to congestion or network element down time. TBD.

4.2.3.7 Trouble tickets forwarding, responsibility, resolutions.

1. When a fault in one domain affects the quality of the neighboring ATN network, the fault must be isolated quickly and the affected neighbors notified immediately. For example, routing problems at a BIS or a faulty process in an end system that generate unacceptable or erroneous packets that will cause congestion in the neighboring ATN must be isolated and the affected neighbor must be notified to clear their buffers.
2. Cross organization communication of faults should be network manager to network manager via the standard means of trouble ticket information exchange.
3. The priority to be given to trouble tickets, based on the type of faults, can be agreed upon between organizations and standardized. Each organization is expected to take appropriate actions to resolve the trouble in an acceptable time. For example, high priority troubles should be handled immediately. This is to localize problems as quickly as possible and to reduce impacts on the quality of the overall ATN network.

4.2.3.8 Configuration coordination.

1. Configuration changes typically affect services and are performed at low-peak hours within a domain. For the global ATN network, low-peak hours will differ from region to region. In coordinating configuration changes, sufficient time is needed to allow the affected organizations to implement the changes.
2. Configuration changes of BIS routers and routing policies need to be coordinated among all the affected organizations. Changes and schedule need to be agreed upon before they are put in effect.
3. Each affected organization evaluates and determines the impact of the configuration

change to its partnering organizations. In turn, each affected organization will initiate configuration change requests to their partnering organizations that will also be affected by the change.

4.2.3.9 Fault monitoring, performance degradation information, traffic information for Customer Network Management (CNM), logging of exchanged messages.

1. When a scheduled outage is to affect ATM service availability, the initiating organization needs to notify the aviation community ahead of time via commonly acceptable means, such as the use of NOTAMs.
2. When source of a detected fault is outside an organization, the source organization needs to be notified in quickly so they can isolate and mitigate the problem.
3. Because of national security and reasons of air safety, direct interaction across organizations for network manager to agent operations is not advised.
4. Each organization is to inform adjacent organization of a ATN network performance degradation that affects that organization. The potential problem, the planned actions, and the time frame for mitigation are shared across organizations. Similarly, ATN performance degradation detected by adjacent organizations is expected to be communicated to the source organization.
5. If a change in ATN network traffic patterns across organizational boundaries is expected, the affected organizations need to be informed.
6. There is no identified need to exchange raw ATN performance data across organizational boundaries on a regular basis. Cross organization manager to agent communication is not necessary and is not advised. If the sharing of raw data is agreed upon between organizations, only data pertaining to those organizations should be shared and not third party data. For example, if raw ATN traffic data is to be exchanged between two organizations, the collected traffic data needs to be processed to eliminate traffic information concerning other organizations. This is to protect and honor organizational privacy and to avoid national security implications.
7. Selective sharing of performance analysis results across organizations based on agreement could help in establishing effective maintenance coordination.

Section 5

Conclusion

This section summarizes key issues addressed in this CONOPS, the proposed guidelines, and next steps for realizing an integrated network management for ATN.

Glossary

A/G	Air/Ground
ACARS	Aircraft Communications Addressing and Reporting System
ACC	Airline Communication Center
ACP	Actual Communication Performance
ADS	Automatic Dependent Surveillance
ADSP	ATN Data Service Provider
AEEC	Airlines Electronic Engineering Committee
AFTN	Aeronautical Fixed Telecommunication Network
AIDC	ATS Interfacility Data Communication
ANP	ATN Network Provider
AOC	Aeronautical Operational Control or Airline Operational Control
APC	Aeronautical Passenger Communication
ARINC	Aeronautical Radio, Inc.
ASE	Application Service Element
ATC	Air Traffic Control
ATIS	Automatic Terminal Information Service
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATNSI	ATN Systems, Inc.
ATS	Air Traffic Service
ATSC	Air Traffic Services Communication
ATSMHS	ATS Message Handling Service
BIS	Boundary Intermediate System
CAA	Civil Aviation Authority
CAASD	Center for Advanced Aviation Systems Development
CM	Context Management
CMU	Communication Management Unit
CNM	Customer Network Management
CNS	Communications, Navigation, and Surveillance
CONOPS	Concept of Operations
CPDLC	Controller Pilot Data Link Communication
ES	End Systems

F2K	Free Flight 2000
FAA	Federal Aviation Administration
FIR	Flight Information Region
FIS	Flight Information Service
G/G	Ground/Ground
GA	General Aviation
GM	Guidance Material
HF	High Frequency
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICP	Installed Communication Performance
IDRP	Inter-Domain Routing Protocol
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
ISO	International Standards Organization
NAS	National Airspace System
NMA	Network Management Agents
NMTF	Network Management Task Force
NOTAM	Notice To Airmen
NSAP	Network Service Access Point
MO	Managed Object
OSI	Open Systems Interconnection
PETAL	
QoS	Quality of Service
RCP	Required Communication Performance
RFC	Request for Comment
RGS	Remote Ground Station
RRI	Router Reference Implementation

SATCOM	Satellite Communications
SARPS	Standards and Recommended Practices
SITA	Societe Internationale de Telecommunication Aeronautiques
SLA	Service Level Agreement
TMN	Telecommunications Management Network
TSAP	Transport Service Access Point
TSEL	Transport Selector
ULA	Upper Layer Architecture
VDL	VHF Data Link
VHF	Very High Frequency