International Civil Aviation Organization
North American, Central American and Caribbean Office (NACC)
GREPECAS CAR Project D – ATN infrastructure in the CAR Region and its ground-ground and ground-air applications
Santo Domingo, Dominican Republic, 27 September 2013

Agenda Item 1: ATN Ground-Ground and Air-Ground Applications
1.2 Review, update, and complete transition plan for the evolutionary development of ATN and applications

REVIEW, UPDATE, AND COMPLETE TRANSITION PLAN FOR THE EVOLUTIONARY DEVELOPMENT OF ATN AND APPLICATIONS

(Presented by FAA)

SUMMARY

This working paper presents the CAR/SAM AMHS Transition Plan and related documents, and invites the Meeting to provide updates to the Plan as necessary.

References:

- Fourth Meeting of the CAR/SAM ATN Task Force (CAR/SAM/ATF/4), Santo Domingo, Dom. Republic, 27 - 28 June 2008
- Fifth Meeting of the ATN Task Force (ATN/TF/05), Mexico City; Mexico, 12 - 13 June 2009
- Sixteenth Meeting of the CAR/SAM Regional Planning and Implementation Group, (GREPECAS/16), Punta Cana, Dominican Republic, 28 March – 1 April 2011

Strategic Objectives	*This working paper is related to Strategic Objectives:* *A. Safety – Enhance global civil aviation safety* *C. Environmental Protection and Sustainable Development of Air Transport*

1. Introduction

1.1 From the 4th ATN Task Force Meeting, modification to the Initial Transition Plan for the Evolutionary Development of the ATN in the CAR/SAM Region were agreed, where this plan shall be the proposal for the ATN in the regions, as well as clear guidance to implement the ATN in the CAR/SAM regions. It was agreed under Conclusion 3/1 that the Initial Transition Plan be modified to incorporate the following documents:

a) Caribbean/South America (CAR/SAM) Regional ATN Ground-to-Ground Transition Plan
b) Caribbean/South America (CAR/SAM) ATN Implementation Plan, and
c) Caribbean/South America (CAR/SAM) AMHS Transition Plan

1.2 During the 4th meeting of the ATN Task Force the group updated the initial Transition Plan for the ATN based on the above mentioned ATN/TF/3 Conclusion 3/1, in which the advances in the guidance material for ATN/IPS (Doc 9896) and the recent publication of ICAO Doc 9880 Part II B for AMHS were considered.

1.3 From the ATN/TF/4 Meeting, it was agreed that the CAR/SAM Regional AMHS Transition Plan will limit its scope to implementing the AMHS and AFTN/AMHS Gateway as specified in ICAO Doc 9880 Part IIB to replace the existing AFTN. It will cover the operational procedures and temporary measures necessary during the transition period. The security and protection of the network will be addressed to prevent AMHS TCP/IP Dedicated Circuits network from interfacing with public internet. During the review of such document the following appendices should be incorporated in the document. Some of the appendices are completed and others have to be developed by the Task Force:

- Appendix I CAR/SAM AMHS Network Status Table
- Appendix II CAR/SAM AMHS Network Backbone Trunks
- Appendix III CAR/SAM TCP/IP v4 Routing Policy
- Appendix IV IPv4 Addressing Scheme
- Appendix V IP Router Interface Control Document
- Appendix VI MTA Routing Policy
- Appendix VII AMHS Address Designation
- Appendix VIII CAR/SAM Directory Service
- Appendix IX AMHS and IP Router Compatibility Test Procedure
- Appendix X AMHS IP Security
- Appendix XI CAR/SAM ATN Task Force Task Assignment
- Appendix XII CAR/SAM AFTN Infrastructure

1.4 During the last meeting of the ATN Task Force (ATN/TF/5), held in Mexico City; Mexico, 12-13 June 2009, the Meeting review the following plans:

- AMHS Transition Plan
- CAR/SAM AMHS Implementation Matrix
- CAR/SAM Backbone of Internetwork G/G ATN Routers
- CAR/SAM ATN Ground / Ground - FASID Table CNS 1Bb
- AMHS IP Routing Policy
- ATN Security Guidance

1.5 With the new structure of the GREPECAS, the CAR D Project was assigned with the desirable for “Plan for the transition of ATN and ATN applications in the CAR Region” as continuation of the former ATN TF, with a target date to complete this updating by **April 2013**.

1.6 ICAO published the Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, and the Aeronautical Telecommunication Network (ATN) Manual for the ATN using IPS Standards and Protocols, Doc 9896 2nd edition, where several topics have evolved and matured as for example the ATN Directory Services (Doc 9880, Part IV — *Security and Systems Management*) and the security requirements for communications in the ATN/IPS, where based on a system threat and vulnerability analysis, IP layer security in the ground-ground ATN/IPS internetwork is implemented using Internet Protocol security (IPsec) and the Internet Key Exchange (IKEv2) protocol.

2. Discussion

2.1 Based on the results from the discussion made during the ATN/TF/5 Meeting, it was agreed that an updated version of the CAR/SAM initial Transition Plan for the ATN, including the CAR/SAM AMHS Transition Plan could be done by the ATN TF. This task is expected to be completed by the end of 2010.

2.2 Since then, the implementation of AMHS in the CAR Region has progressed at a steady pace, and ATN routers have been implemented. The Plan needs to be reviewed and amendment to complete the deliverable, as well as focused on the CAR Region experience and requirements:

- Appendix A: AMHS Transition Plan- draft
- Appendix B: AMHS IP Routing Policy
- Appendix C: IP Router- ICD
- Appendix D : ATN Security Guidance Document

3. Suggested Actions

3.1 The meeting is invited:

a. review the draft plan for the AMHS Transition and amend it as needed considering the maturity of ICAO guidance material and AMHS learned lessons;
b. analyse the original assignment for the transition plan for the evolutionary development of ATN and applications; and
c. provide updates as needed.

— — — — — — — — — — —

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

INTERNATIONAL CIVIL AVIATION ORGANIZATION
(ICAO)

CARIBBEAN AND SOUTH AMERICA REGION

AIR TRAFFIC SERVICE MESSAGE HANDLING SYSTEM (AMHS)

TRANSITION PLAN

DRAFT

SUMMARY

This document presents a plan for the AMHS transition activities applicable to the CAR/SAM Region and provides information on the ground infrastructure required to support the Aeronautical Message Handling System (AMHS) service. The AMHS Transition Plan is a prime document that details the transition strategy from Aeronautical Fixed Telecommunication Network (AFTN) to an AMHS environment. This Transition Plan will address the recommendations to overcome various obstacles such as network incompatibility between ICAO regions, timely coordination and management of AMHS addressing, security management, and the upgrading of regional telecommunication backbone network.

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

Table of Contents

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

LIST of FIGURES

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

LIST of TABLES

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

EXECUTIVE SUMMARY

This document presents a plan for the AMHS transition activities applicable to the CAR/SAM Region and provides information on the ground infrastructure required to support this transition. The use of AMHS over TCP/IP for this region has been adopted by the CAR/Sam Regional ATN Task Force. The AMHS Transition Plan is a prime document that details the transition strategy from Aeronautical Fixed Telecommunication Network (AFTN) to an AMHS environment. This Transition Plan will address the recommendations to overcome various obstacles such as network incompatibility between ICAO regions. Timely coordination and management of the AMHS addressing scheme, upgrading of backbone circuits and the network along with security management is necessary due to the dynamics of the network in relation to the "store and forward" function of the fixed service of AFTN.

1.0 INTRODUCTION

1.1 PURPOSE

The CAR/SAM AMHS Transition Plan is designed to provide the roadmap to implement the AMHS over TCP/IP in the CAR/SAM Region. Once the ICAO CAR/SAM Regional ATN Task Force completes the CAR/SAM AMHS Transition Plan, it must be adopted by the ICAO GREPACAS CNS/ATM. It is considered base-lined and shall not be modified. Any modification of this transition plan shall be developed by the Task Force and adopted by ICAO GREPACAS CNS/ATM. The Appendices as depicted under Section 1.4 shall be allowed to be modified and updated accordingly. The scope of all documents depicted in Section 1.5 is designed to achieve the goals and objectives set by this ICAO CAR/SAM AMHS Transition Plan.

1.2 OBJECTIVE

The objective of this document is to provide guidance and information on transition activities that will need to occur for the CAR/SAM Region to migrate from AFTN to AMHS.

1.3 OVERVIEW

This document presents general information and recommendations for AMHS transition activities within the CAR/SAM Region.

1.4 SCOPE

The CAR/SAM Regional AMHS Transition Plan will limit its scope to implementing the AMHS and AFTN/AMHS Gateway to replace the existing AFTN. It will cover the operational procedures and temporary measures necessary during the transition period. The security and protection of the network will be addressed as the TCP/IP network protocol can interface directly with the Public Internet through its regional AMHS Virtual Private Network (VPN).

1.5 REFERENCE DOCUMENTS

Internet Protocol Suite (IPS) Standards and Recommended Procedure (SARP) (Draft version)
Manual of Technical Provision for the ATN-ICAO Doc. 9705 3rd Edition
ICAO Location Indicators – ICAO Doc 7910
ICAO Annex X
ICAO CNS Facilities and Services Implementation Document (FASID)
CAR/SAM ATN Plan
ICAO Asia/Pacific Regional ATN Router Routing Policy
ICAO Asia/Pacific Regional ATN Router Interface Control Document (ICD)
ICAO Asia/Pacific Regional Message Transfer Agent (MTA) ICD

1.6 APPENDIX LISTING

Appendix I	CAR/SAM AMHS Network Status Table
Appendix II	CAR/SAM AMHS Network Backbone Trunks
Appendix III	CAR/SAM TCP/IP v6 Routing Policy
Appendix IV	IPv6 Addressing Scheme
Appendix V	IP Router Interface Control Document
Appendix VI	MTA Routing Policy
Appendix VII	AMHS Address Designation
Appendix VIII	CAR/SAM Directory Service
Appendix IX	AMHS and IP Router Compatibility Test Procedure
Appendix X	AMHS VPN Security
Appendix XI	CAR/SAM ATN Task Force Task Assignment
Appendix XII	CAR/SAM AFTN Infrastructure

2. BACKGROUND

2.1 CONSTRAINTS

2.1.1 Industry has been using TCP/IP version 4 since late 1980s and many Civil Aviation Authorities (CAAs) and airline related service providers have used TCP/IP to communicate with and among one another. The ICAO Aeronautical Telecommunication Panel (ATNP) based on Open System Interface (OSI) protocol, was created in mid-1990 to provide a seamless network for ATC service between CAAs and the airlines. The ATNP was merged into the Aeronautical Communication Panel (ACP) and became the ACP Working Group N (WG-N) (Network). ACP WG N has developed an IPS SARP based on TCP/IP as an extension of the ATN OSI based system.

2.1.2 As the CAR/SAM region becomes the first ICAO region to fully comply with the IPS SARPs, the following issues should be considered:

- The IPS SARPs will not be finalized before 2008
- The Technical Manual for the IPS has not been completed
- The Guidance Material has not been considered

- The IPS SARPs do not address the correlation between other implementation documents
- IPS SARPs refers only to various industry RFCs without a Profile. This will require extensive coordination with other ICAO regions to insure network compatibility
- The Air-Ground network protocol has not been finalized even though the IPS SARPs seem to imply all services have been addressed.

2.2 EXISTING AFTN INFRASTRUCTURE

2.2.1 Currently there are over 100 international AFTN circuits that operate within the region and between adjacent regions. The AFTN network is primarily based on dedicated point-to-point connections, either by dedicated circuits or dedicated channels, with a normal bandwidth of up to 9.6 Kbps based on X.25 network protocol. There are a number of low speed AFTN circuits operating at 50 bps either with no network protocol or COPB or asynchronous protocol. The detail CAR/SAM AFTN Infrastructure is shown in Appendix XI CAR/SAM AFTN Infrastructure

2.3 AFTN OPERATION

2.3.1 ICAO Annex X describes AFTN as a service based on the "store and forward" function for conveyance of text messages using character-oriented procedures. AFTN messages are forwarded on a hop-by-hop basis using pre-configured routes that are the most expeditious to affect delivery to the addressee. This means messages are routed by the application (AFTN switch) not by the network router. This operation is required so that messages exchanged between adjacent AFTN centers, including transit messages, are processed, stored and forwarded to the next AFTN center until the messages have reached their intended destination.

2.3.2 AFTN has diversion routing lists agreed to by the administrations operating the communication centers where the AFTN switches reside. These lists are statistically configured and used to immediately reroute traffic in the event of a circuit outage in a fully automatic communication center or to manually reroute traffic within 10 minutes in a non-fully automatic communication center. Under AFTN procedures, the sending station will hold messages transmitted, and in the event that continuity of message traffic is not maintained, they are re-transmitted. Continuity of message traffic is supervised by using sequence numbers applied to all traffic over a particular channel. The AFTN system is depicted in Figure 1.

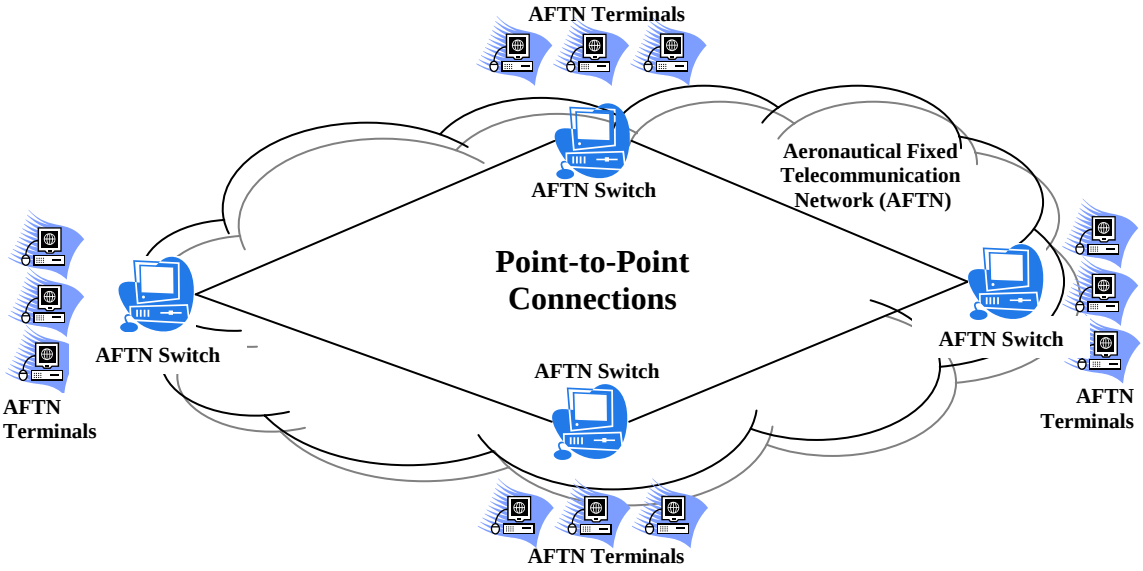


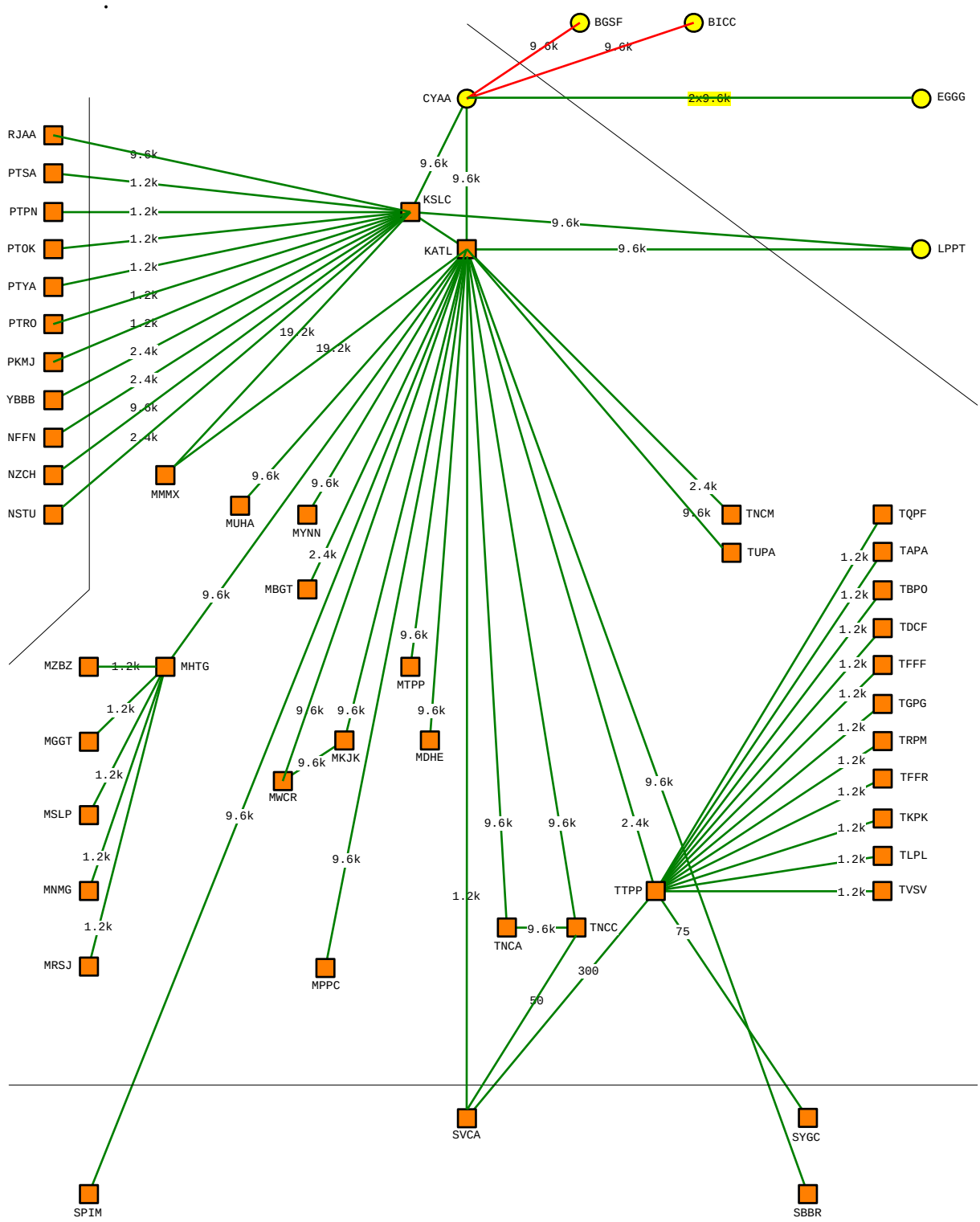
Figure 1 – AFTN System

2.3.3 The procedure for tracking of unknown or lost messages has been refined over the years. It requires the AFTN centers to manually contact one another to resolve problems. These problems can be easily traced through the dedicated X.25 port to determine the source of the lost or unknown messages to either the sending or receiving AFTN center.

2.3.4 The following charts (NAM/CAR and SAM) and location tables show the current topology and portray the platform and baseline upon which the transition to CAR/SAM AMHS is based.

Note: The North American (NAM) Region is included in the chart due to its extensive connection with the Caribbean Region (CAR).

NAM/CAR COM Chart

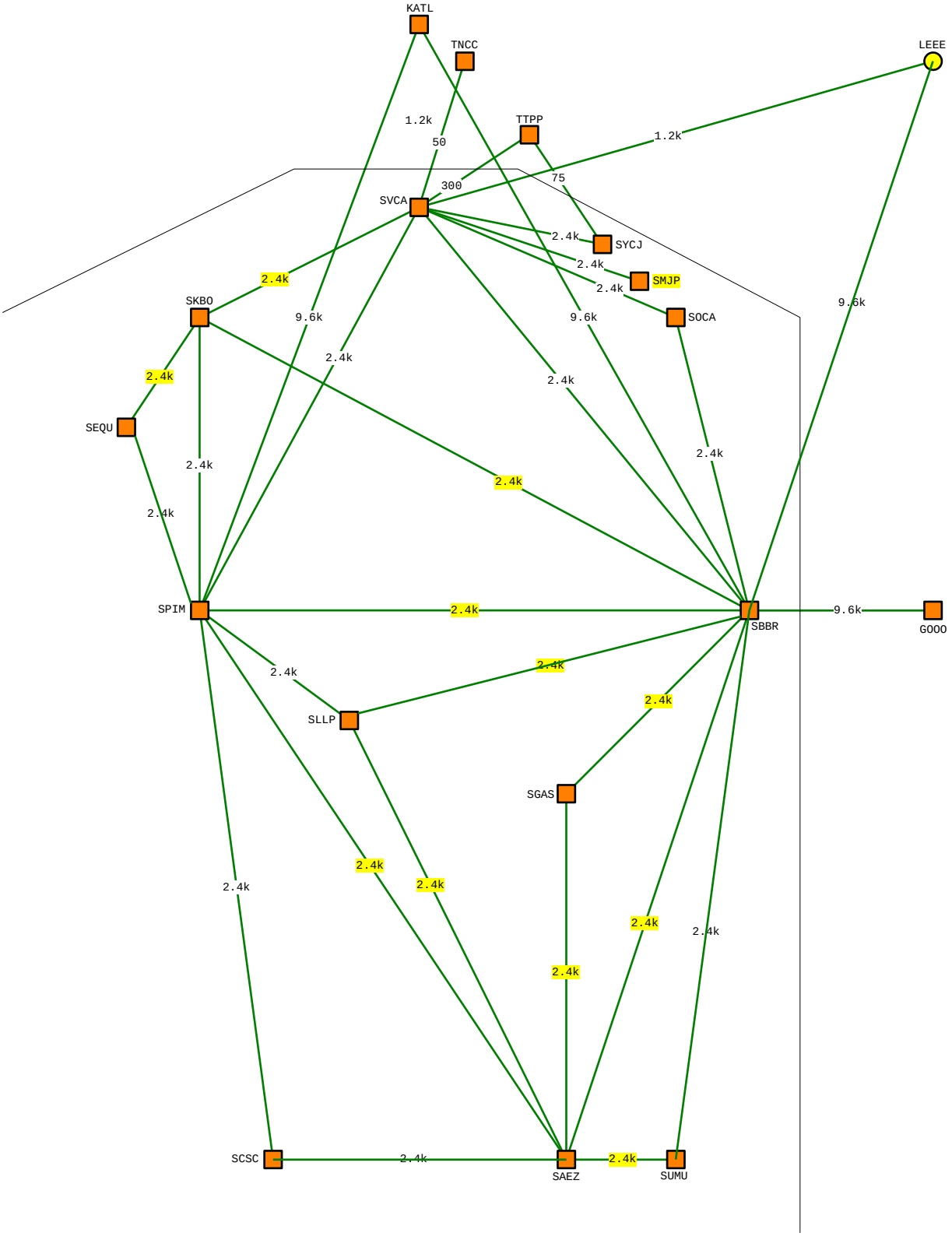


CIDIN/AFTN COM Centre
AFTN COM Centre
9.6k CIDIN Link with Line Speed
1.2k AFTN Link with Line speed

12-04-06 R.E.Wagner
AFTN: EHAMYTYX
E-mail: r.e.wagner@lvnl.nl

APPENDIX A
DRAFT – AMHS Transition Plan - DRAFT

SAM COM Chart



12-04-06 R.E.Wagner
AFTN: EHAMYTYX
E-mail: r.e.wagner@lvnl.nl

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

Listed in alphabetical order by State/Territory Name

State/Territory	Location Indicator	Location Name
Anguilla Island	TQPF	Anguilla
Antigua and Bermuda	TAPA	Antigua
Aruba	TNCA	Oraniestad
Bahamas	MYNN	Nassau
Barbados	TBPO	Bridgetown
Belize	MZBZ	Ph.S.W.Goldson
Canada	CYAA	Ottawa
Cayman Islands	MYCR	Grand Cayman
Costa Rica	MRSJ	San Jose
Cuba	MUHA	Habana
Dominica	IDCF	Dominica
Dominican Republic	MDHE	Santo Domingo
El Salvador	MSLP	San Salvador
French Antilles	TFFF	Fort de France
French Antilles	TFFR	Pointe a Pitre
Grenada	TGPG	St Georges
Guatemala	MGGT	Guatemala
Haiti	MTPP	Port-au-Prince
Honduras	MHTG	Tegucicaba
Jamaica	MKJK	Kingston
Mexico	MMMX	Mexico
Montserrat	TRPM	Plymouth
Netherlands Antilles	TNCC	Curacao
Nicaragua	MNMG	Managua
Panama	MPPC	Panama
Puerto Rico	TJSJ	San Juan
St. Kitts and Navis	TKPK	St. Kitts
St. Lucia	TLPL	St. Lucia
St. Vincent and the Grenadines	TVSV	St. Vincent
Trinidad and Tobago	TTPP	Piarco
Turks and Caicos Islands	MBGT	Grand Turk
United States	KATL	Atlanta
United States	KSLC	Salt Lake City
Virgin Islands	TUPA	Tortola

APPENDIX A

DRAFT – AMHS Transition Plan - DRAFT

Listed in alphabetical order by COM Centre Location Indicator

Location Indicator	Location Name	State/Territory
CYAA	Ottawa	Canada
KATL	Atlanta	United States
KSLC	Salt Lake City	United States
MBGT	Grand Turk	Turks and Caicos Islands
MDHE	Santo Domingo	Dominican Republic
MGGT	Guatemala	Guatemala
MHTG	Tegucigalpa	Honduras
MKJK	Kingston	Jamaica
MMMX	Mexico	Mexico
MNMG	Managua	Nicaragua
MPPC	Panama	Panama
MRSJ	San Jose	Costa Rica
MSLP	San Salvador	El Salvador
MTPP	Port-au-Prince	Haiti
MUHA	Habana	Cuba
MYCR	Grand Cayman	Cayman Islands
MYNN	Nassau	Bahamas
MZBZ	Ph.S.W.Goldsor	Belize
TAPA	Antigua	Antigua and Bermuda
TBPO	Bridgetown	Barbados
TDCF	Dominica	Dominica
TFFF	Fort de France	French Antilles
TFFR	Pointe a Pitre	French Antilles
TGPG	St Georges	Grenada
TJSJ	San Juan	Puerto Rico
TKPK	St. Kitts	St. Kitts and Nevis
TLPL	St. Lucia	St. Lucia
TNCA	Oranjestad	Aruba
TNCC	Curacao	Netherlands Antilles
TQPF	Anguilla	Anguilla Island
TRPM	Plymouth	Montserrat
TTPP	Piarco	Trinidad and Tobago
TUPA	Tortola	Virgin Islands
TVSV	St. Vincent	St. Vincent and The Grenadines

3. TRANSITION PLAN

The AMHS will be gradually implemented without impact to the operation of existing AFTN services to States or organizations (airlines, service providers, etc.).

3.1 NETWORK

3.1.1 The ICAO Doc. 9705 recommends two options for the establishing of an AMHS internet and the IPS SARPs recommend TCP/IP as another alternative.

- ATN Router using X.25 subnet: ICAO Asia/Pacific has adopted this network protocol as their ATN Internet.

- ATN Router using IP subnet: (requires SNDCF). The ATN IP subnet with SNDCF will be able to utilize the IP network (TCP/IP) but requires another ATN IP Subnet to receive the message due to Inter-Domain Routing Protocol (IDRP) encapsulated in the message.

3.1.2 The draft version of the IPS SARPs recommends using the TCP/IP for AMHS Ground-Ground Internet. The ICAO CAR/SAM Region has adopted this approach and tasked the CAR/SAM ATN Task Force to develop the plan to implement this network to support the AMHS.

3.1.3 ICAO European Region has also adopted this approach but using IPv4 as the interface with their AMHS and encapsulating the IPv4 messages into the IPv6 backbone. These messages will be converted back to IPv4 when received at the end destination (tunneling).

3.1.4 Some ICAO regions have selected the ATN ICS as the underlying AMHS network protocols (CLNP/TP4) while other regions have selected IPS-based networks for the AMHS. The use of different network protocols in different regions means that the direct communications between any MTA to any other MTA is not possible across all ICAO regions. Direct MTA to MTA communications is only possible where the MTAs are on networks using the same communication protocols. In those cases where different regions are using different network protocols, an AMHS MTA must act as the relay between the different networks. Appendix III CAR/SAM TCP/IP v6 Routing Policy AMHS/MTA and Appendix VI MTA Routing Policy will specify the resolution of the network incompatibility without any system modifications.

3.1.5 When reviewing the current AFTN topology, a majority of AFTN circuits will not be suitable to be used for AMHS without some form of upgrade. These upgrades will need to be in the form of high-speed links (bandwidth capacity) with protocols compatible with the lower layers. The bandwidth requirements for an AMHS MTA are higher and will require the State to upgrade their circuits to a minimum of 64Kbps. For those States and/or sites that do not require an MTA, a User Agent (UA) can be connected to a remote MTA using a 9.6Kbps circuit. It may also be possible to install an AMHS MTA with a limited number of connections and low traffic volumes using a

9.6Kbps circuit. States selecting the low-speed MTA option must be able to upgrade the circuit if traffic loading increases above 40% of circuit capacity.

3.1.6 As a justification for the circuit speeds, a comparison of the number of bytes transmitted using AFTN and AMHS for the same size message. Using a typical message size of 250 characters, the AMHS shows an increase on average of at least 100%. This is due to the generated AMHS message overhead. This is particularly true for small messages because as the message size increases the amount of overhead generated is less significant to the size of the body of the message.

Comparison of X.25 Message Sizes Using AFTN and AMHS
(Results courtesy of the INCA[1] Project.)

Data Set #	Set # 1	Set # 2	Set # 3	Set # 4
Size of user message (A)	42	255	7480	13
AFTN				
Size of complete message including overheads **(B)**	98	311	7845	N/A
Size of total data transported - user data **= (B) - (A)**	56	56	365	N/A
Ratio of user message / total message size (%) **= (A)/(B) %**	42.86%	81.99%	95.35%	N/A
AMHS				
Size of complete message including overheads and delivery report **(C)**	4231	4448	12783	4271
Size of total data transported - user data **= (C) - (A)**	4189	4193	5303	4258
Ratio of user message / total message size (%) **= (A)/(C) %**	0.99%	5.73%	58.52%	0.30%
AMHS vs. AFTN				
Ratio of total AFTN / total AMHS (%) **= (B) / (C) %**	2.32%	6.99%	61.37%	N/A
Ratio of total AMHS / total AFTN **= (C) / (B)**	43.17	14.30	1.63	N/A

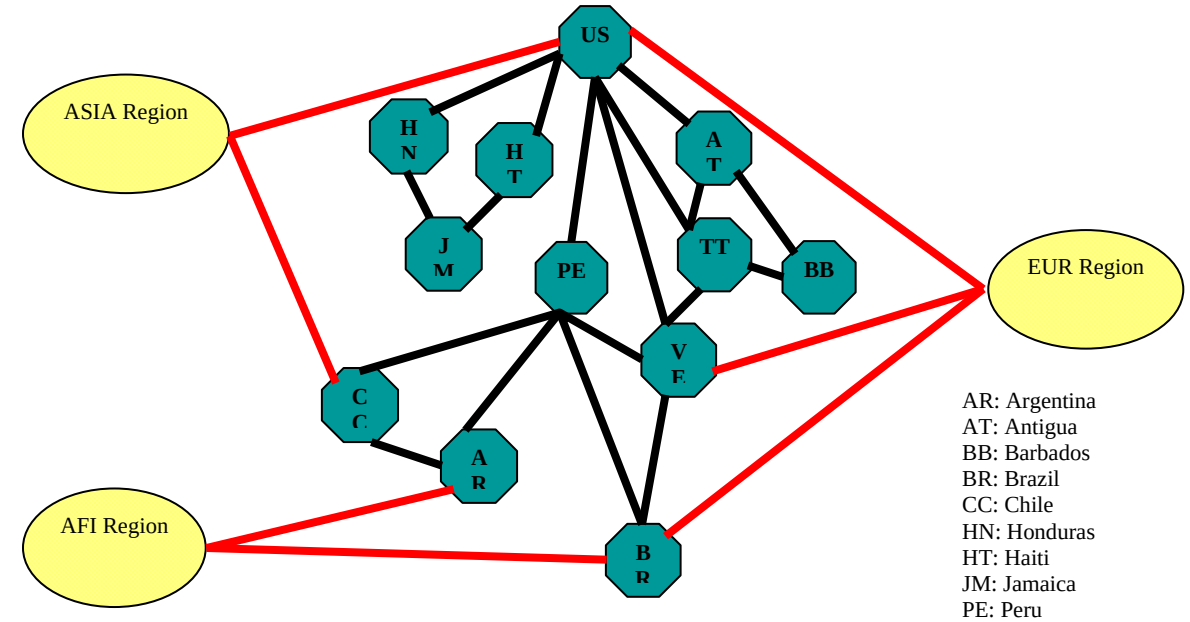
Table 3. X.25 Message Sizes Using AFTN and AMHS

3.1.7 Any existing AFTN circuits that are close to or exceeding 40% load during peak hours should be prioritized to increase their bandwidth due to AMHS headers and possible alternative traffic. It is important to also note that costs will increase due to implementing higher bandwidth links. Therefore, the region should review its requirements in having to use point-point circuits everywhere when a number of

[1] INCA (Investigation of Networked CNS/ATM Applications) project was a joint Airservices Australia and Airsys ATM Pty Ltd ATN research and development program, which investigated the AMHS during 1999/2000.

strategically placed links offering alternate routing between key sites may suffice. This may help to offset the costs and still provide for an efficient ground-ground network for the AMHS. States will need to ensure that not only the links that are established between States are capable of transferring data in a timely manner but also they must insure that those links that provide an alternate path for use in times of primary links disruption are also capable of transferring data in a timely manner.

3.1.8 The network backbone depicted below is for a preliminary AMHS over TCP/IP Routing Network. The AMHS Backbone tries to use existing trunks that have already been established between nominated States who will operate the backbone that is currently used by AFTN. Further refinement of this network architecture is required based on the latest update of the regional telecommunication network. As part of the transition from AFTN to the AMHS, the existing link capacity, especially those using X.25, must be able to handle both AFTN and AMHS for those States who do not intend to migrate to AMHS immediately. It is assumed that States that have been nominated to provide the AMHS backbone routing environment will do so in a timely manner so as to allow those States who are ready to start their implementation programs can do so without experiencing too much restriction within the region. Where a nominated State cannot provide the AMHS backbone then an alternative arrangement should be put in place for another State, who is willing to provide the service.



3.2 CAR/SAM Regional AMHS Major Hubs: The States should meet all criteria as specified below to be considered as a major network backbone in the CAR/SAM region:

- Have a minimum of one connection to other ICAO regions
- Have a minimum of two connections within the region
- Have high speed circuits that are capable of handling high volume traffic including alternative routing of traffic
- Have an AMHS and AMHS/AFTN Gateway
- Be staffed 24 hours, 365 days a year

3.3 ATS Message Handling System (AMHS): The message handling service provided in the ATN is called the *ATS Message Handling Service (ATSMHS)*. This service is specified using X.400 standards following the X.400 architecture described above. There are two levels of ATSMHS service: Basic ATS Message Service and Extended ATS Message Service.

3.4 Basic ATS Message Service provides, from a user perspective, a nominal capability equivalent to that provided by AFTN.

3.5 Extended ATS Message Service provides enhanced features such as supporting transfer of more complex message structures, use of the directory service, and support for security.

3.5.1 ICAO Doc 9705 distinguishes the service from the set of computing and communication resources implemented by ATS organizations to provide the ATS message handling service. The set of computing and communication resources is called the *ATS Message Handling System (AMHS).* For Basic ATS Message Service, the following AMHS entities are defined:

- **ATS Message Server** - An X.400 MTA and optionally one or more MSs

- **ATS Message User Agent** – An X.400 UA designed to replace the AFTN Terminals

- **AFTN/AMHS Gateway** – An MTA and an AFTN specific AU, called a Message Transfer and Control Unit (MTCU) with corresponding Control Position.

- **CDIN/AMHS Gateway** – An MTA and a CDIN specific AU, called a Message Transfer and Control Unit (MTCU) also with a corresponding Control Position.

3.5.2 The European Region has adopted the use of AMHS/AFTN Gateway option to support their connection with Asia/Pacific region. The European Region will use AMHS for Intra-region communication bypassing the use of the CIDIN/AMHS Gateway.

3.6 Initial AMHS Configuration

3.6.1 Figure 5 depicts the initial AMHS configuration. In this configuration the AFTN system is still in place, a supporting network of TCP/IP Routers and AFTN/AMHS Gateways are introduced to begin the transition to AMHS. In this configuration, basic ATS message service is provided. From a user's perspective, there should be no difference from the AFTN only environment at an AFTN terminal. The advantage of the AMHS is that the TCP/IP routers of the AMHS perform re-routing automatically without the need for preconfigured diversion routing list thus permitting direct MTA-to-MTA routing rather than having messages relayed through an intervening MTA.

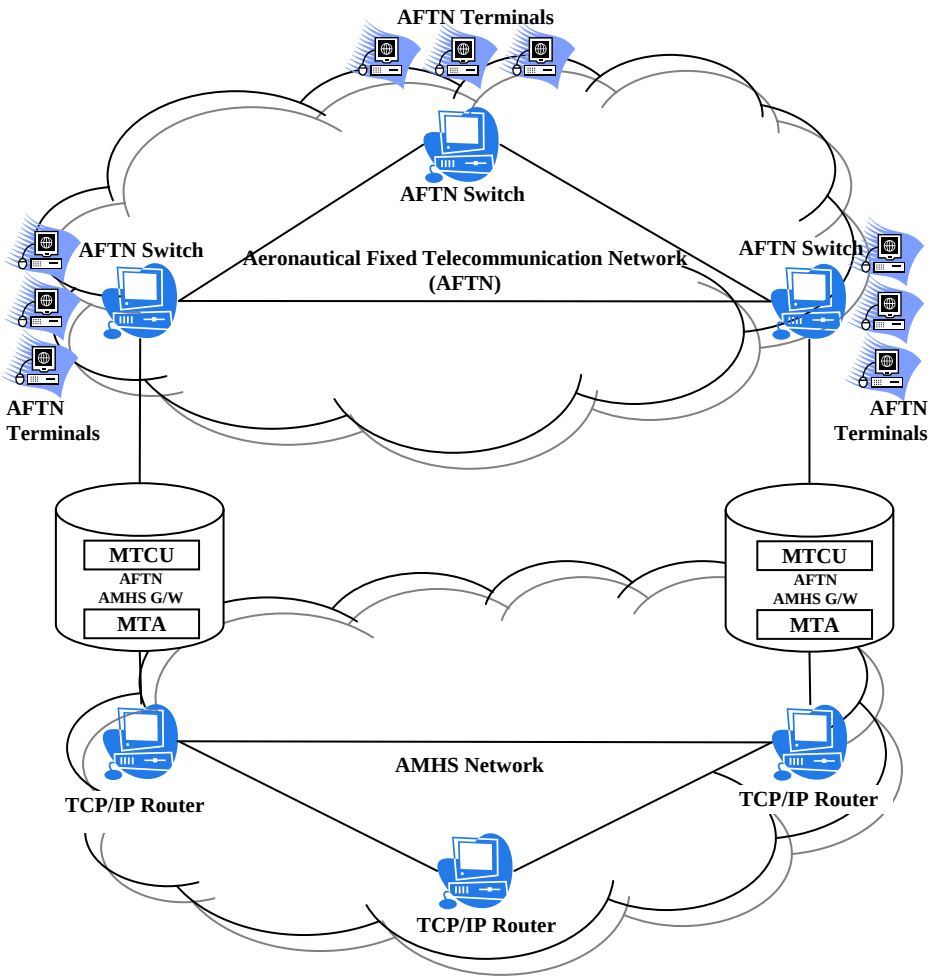


Figure 5. – Initial AFTN-AMHS Gateway System

3.7 Evolving AMHS Configuration

3.7.1 Figure 6 depicts the evolving AMHS configuration. In this diagram AFTN terminals and associated AFTN switches are still in place to accommodate administrations that have not yet switched to AMHS. The evolving system now has AMHS terminals. These terminals have ATS message user agents embedded in them. The AMHS user terminals interface to ATS Message Servers, which as described above, will have an MTA to interface the MTA and most likely an embedded MS capability to permit storage of messages when terminals are not in-use. Administrations may introduce AMHS terminals while at the same time maintaining AFTN terminals. In this case, it is likely that a combination AFTN/AMHS Gateway and ATS Message Server will be employed. It is anticipated that gateway vendors will provide this upgrade path.

3.7.2 The States currently with AFTN/MET terminal should consider replacing the terminal with an UA or keep their AFTN/MET terminal connected to the AFTN/AMHS Gateway. The UA is recommended for States with only one connection and low traffic volume to minimize operating cost.

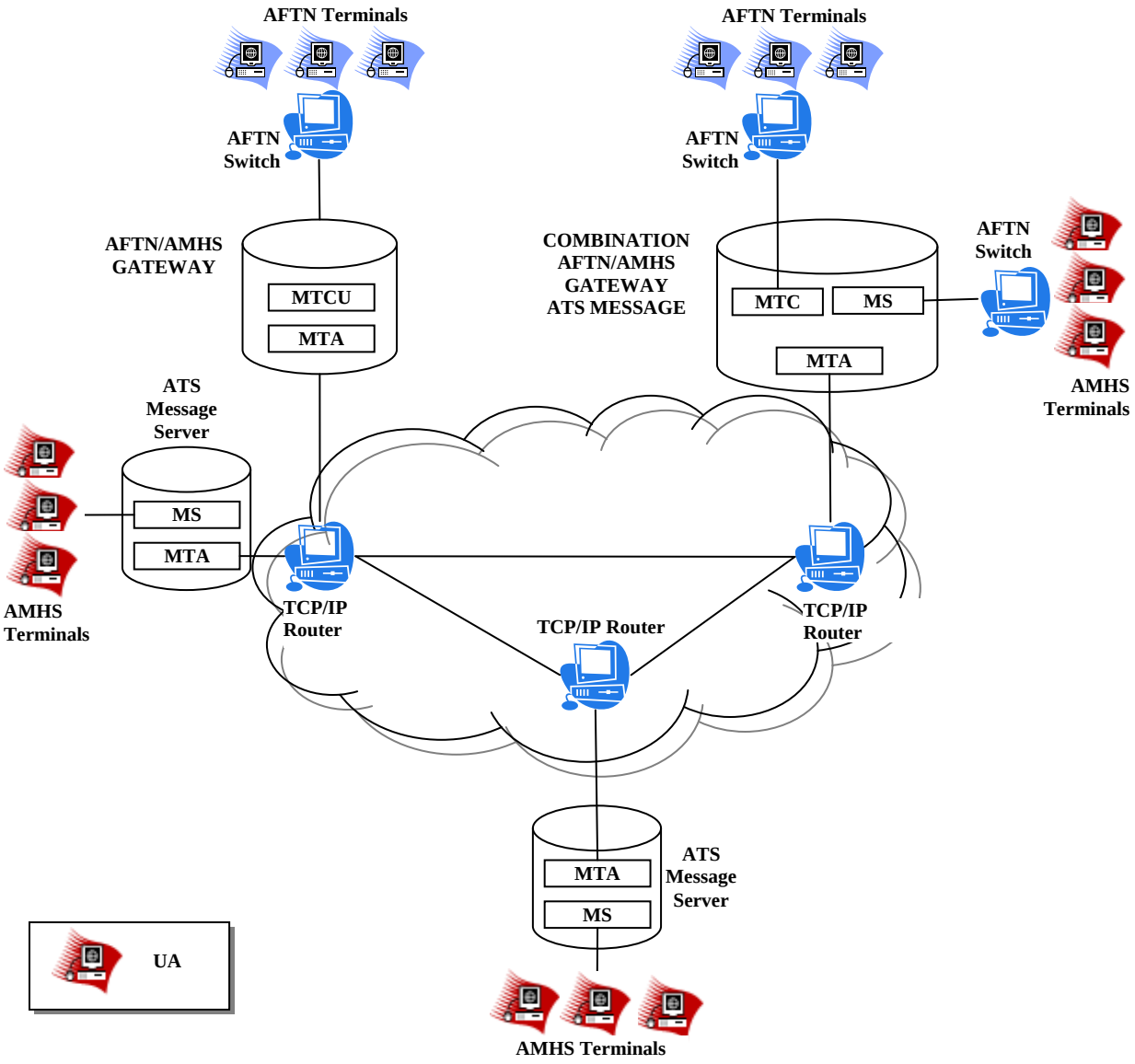


Figure 6 – Evolving AMHS System

3.8 MTA Routing Policy

3.8.1 The MTA routing policy is required to govern the message exchange within the region as well as Inter-region message traffic. The ICAO Doc. 9705 specifies the End-State ATN environment where all States would have AMHS or an UA. It is critical to adhere to the MTA routing policy as well. This will provide the TCP/IP Routing Policy and AMHS Address Management the necessary coordination to prevent network breakdown due to message rejection alerts because of unknown AMHS addresses or unknown routing addresses.

3.8.2 The MTA Routing Policy as depicted in Appendix VI will address the following issues:

- Intra-Region MTA routing during the AFTN/AMHS transition period: Specify the AMHS MTA address control policy during the transition between AFTN and AMHS

- Intra-Region MTA routing at End-State Environment: Specify the AMHS MTA address control policy in the End-State Environment

- Inter-Region MTA Routing during transition period: Specify the AMHS MTA address control policy during the transition of the AFTN/AMHS environment as well as different network protocols

- Inter-Region MTA Routing at End-State Environment: Specify the AMHS MTA address control policy at the End-State environment. It is noted that due to network protocol incompatibility, the transition period may be extended for a long period.

3.9 AMHS/AFTN GATEWAY

3.9.1 AMHS/AFTN Gateway is utilized during the transition to ensure the seamless transition between the AFTN and AMHS. The AMHS/AFTN Gateway is designed to interface with end-systems as well as other switches (e.g. AFTN switch, AFTN terminal, AMHS or AMHS/AFTN Gateway). The AFTN/AMHS Gateway is limited to a transitional period and therefore is not included in the ATN End-State environment.

3.10 DIRECTORY SERVICE

3.10.1 The Directory Service as specified in the ICAO Doc. 9705 is based on a X.500 platform and would require extensive coordination for an entire ATN network (Air-Ground and Ground-Ground services) The immediate issue under this Directory Service is the managing and timely coordination of the AMHS addresses as States begin to operate the AMHS in addition to their AFTN operation. The AMHS address management includes all the coordination necessary to inter-act with other ICAO regions.

3.11 OPERATION PROCEDURE (to be developed)

3.12 SECURITY

3.12.1 A key element of the CAR-SAM regional transition to AMHS is Information Security. This is especially true because CAR-SAM will operate with TCP/IP protocols. The region should have a work program in place that includes policy, guidance, and an implementation strategy.

3.12.2 Security Policy - The CAR-SAM region should adopt an overall Security Policy. The security policy essentially requires that each state designate an individual or

organization that is responsible for security. The individual/organization will be required to ensure that appropriate controls are in place to protect system data, services, and resources from both unintentional defects and deliberate attack. The Asia/Pacific System Integrity Policy may be used as a guide.

3.12.2 Security Checklist - In order to support the Security Policy in a consistent manner throughout the region a security checklist which identifies a minimal set of management, technical, and operational controls should be developed. The checklist may be thus used by an administration to support verification of the Security Policy. This checklist may be derived from general standard assessment guides and/or from guides that administrations may already have in place.

3.12.3 Security Implementation Plan - It is proposed that a Security Implementation Plan be developed that identifies the planned implementation of controls on a system-wide basis. In particular, the plan should identify what controls will be implemented in order to support the evolving ATN applications and the evolving ATN architecture in the CAR-SAM region. A possible evolution of technical security controls could be as follows:

- Technical controls will initially consist of securing router connections on a point-to-point basis. This could be with router specific mechanisms with pre-shared keys.
- A basic incident response capability could be introduced.
- Basic firewalls and other security appliances may also be introduced.
- As the IP is deployed on a larger basis, a Virtual Private Network (VPN) using common techniques such as IPsec could be employed.
- As the AMHS evolves to enhanced services, including directory services, AMHS application security will be employed
- It is expected that as the system expands manual key management techniques will not be sufficient and a Public Key Infrastructure (PKI) will be deployed.
- Eventually an enhanced incident response capability will be needed.

Operational and Management controls such as key management policies, procedures, etc. must also evolve. The Security Implementation Plan will identify the phasing of all security controls throughout the CAR-SAM system.

3.12.4 Supporting Security Documentation - Several system-wide documents should be developed to support implementation of security provisions in the CAR-SAM region. The following minimal set is proposed.

System-Wide Risk Assessment The assessment would identify common AMHS resources and examine the risk (likelihood and impact) in terms of the general security goals of confidentiality, data integrity, and availability.

System-Wide Contingency Plan A system-wide contingency and disaster recovery plan be developed. This plan would identify the coordination activities, processes, and procedures to be followed in the event that an AMHS system is unavailable.

System-Wide Incident Response Plan The plan would specify common procedures for identifying, reporting, and responding to computing incidents.

Security Technical Guidance Document A security guidance document would provide background information and recommended practices primarily to support the Security Implementation Plan.

4.0 RECOMMENDED ACTIONS

4.1 Finalize the CAR/SAM ATN Transition Plan
4.2 Update the CAR/SAM Regional Telecommunication Major Hub Backbone
4.3 Identify the Communication Centers that require AMHS or UA only
4.4 Identify the circuits that need to be upgraded
4.5 Develop waterfall schedule for transition for an entire region
4.6 Evaluate the IPv6 versus IPv4 due to compatibility issue with European region
4.7 Obtain IP address scheme (States obtain the address individually or the Regional ICAO to designate the address for the whole region)
4.8 Develop Implementation Documents
4.9 Develop Network Operation Procedure
4.10 Establish an entity to manage the AMHS addressing scheme and coordinate this work with other ICAO regions
4.11 Maintain the CAR/SAM ATN Task Force Task Assign

ACRONYMS

AAC	Aeronautical administrative communication
ACP	Aeronautical Communication Panel
AFTN	Aeronautical Fixed Telecommunication Network
AFTN/MET	Aeronautical Fixed Telecommunications Network/Meteorological
AMHS	Air Traffic Service Message Handling System
AOC	Aeronautical Operational Control
APC	Aeronautical Passenger Communication
ATC	Air Traffic Control
ATN	Aeronautical Telecommunication Network
ATNP	Aeronautical Telecommunication Panel
ATS	Air Traffic Service
ATSC	ATS Communication
ATSMHS	ATS Message Handling Service
CAAs	Civil Aviation Authorities
CAR/SAM	Caribbean and South America
CIDIN	Common ICAO Data Interchange Network
CNS/ATM	Communications, Navigation, and Surveillance Air Traffic Management
CLNP	Connectionless Network Protocol
CAAS	Common AMHS Addressing Scheme
COPB	Common Operational Picture Bridge
DUA	Directory User Agent
ES	End system
FASID	Facilities and Services Implementation Document
G/G	Ground-Ground
GREPECAS	Caribbean/South American Regional Planning and Implementation Group
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
IDRP	Inter-Domain Routing Protocol

IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPS	Internet Protocol Suite
IPM	Interpersonal Messaging
IS	Intermediate System
ISO	International Standardization Organization
ISP	International Standardized Profiles
MS	Message Store
MTA	Message Transfer Agent
MTCU	Message Transfer and Control Unit
MTS	Message Transfer System
OSI	Open System Interface
RFC	Requests for Comments
SARPs	ICAO Standard and Recommended Practices
SNDCF	Sub Network Dependent Convergence Function
UA	User Agent
VPN	Virtual Private Network

APPENDIX B

INTERNATIONAL CIVIL AVIATION ORGANIZATION
CARIBBEAN AND SOUTH AMERICA OFFICE

(Presented by USA/FAA)

INTERFACE CONTROL DOCUMENT FOR AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) GROUND-GROUND ROUTER IN THE CARIBBEAN AND SOUTH AMERICA REGIONS

VERSION 0.1

APPENDIX B

CONTENTS

LIST OF FIGURES

FIGURE **PAGE**

APPENDIX B

1.0 SCOPE

This document provides ATN Ground to Ground router ICD guidelines for the routers that form nodes of the CAR/SAM regional network Backbone. This ICD addresses the Physical, Link, and Internet layers of the ATN G/G router using the TCP/IP model.

1.1 Reference Documents

The following documents are reference documents applicable to the CAR/SAM Regional Router ICD for ATN G/G Router. These documents do not form a part of this ICD and are not referenced within the document.

1.2 Applicable Documents

The following documents form a part of this ICD to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this ICD, the contents of this ICD shall be the superseding requirements

1.2.1 Internet Standards

RFC-791 Internet Protocol, September 1981
RFC-796 Address Mappings, September 1981
RFC-793 Transmission Control Protocol, September 1981
RFC 894 Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
RFC-2464 Transmission of IPv6 Packets over Ethernet Networks, December 1998
RFC-2427 Multiprotocol Interconnect over Frame Relay (FR), September 1998
RFC-2590 Transmission of IPv6 Packets over Frame Relay Networks Specification, May 1999
RFC-2460 Internet Protocol, Version 6 (IPv6) Specification, December 1998
RFC-2373 IP Version 6 Addressing Architecture
RFC-950 Internet Standard Subnetting Procedure, August 1985
RFC-2784 Generic Routing Encapsulation (GRE), March 2000
RFC-2473 Generic Packet Tunneling in IPv6 Specification, December 1998
RFC-3168 The Addition of Explicit Congestion Notification (ECN) to IP, September 2001

APPENDIX B

2.0 INTERFACE DESIGN CHARACTERISTICS

This section provides the general functional and physical design characteristics for the interfacing communication devices.

2.1 General Characteristics

The ATN G/G routers are Commercial of the Shelf (COTS) routers that can be easily procured and implemented. The use of these routers with a TCP/IP implementation of the Automatic Message Handling System (AMHS) (RFC1006) will tremendously decrease the time of deployment and final implementation of the AMHS in the CAR/SAM regions.

2.1.1 Protocol Implementation

The general requirements for the ATN G/G router cover the lower three layers of the TCP/IP four-layer model. The TCP/IP model defines a four-layer network model as shown in Figure 1-2. Only the lower three layer is cover under this document.

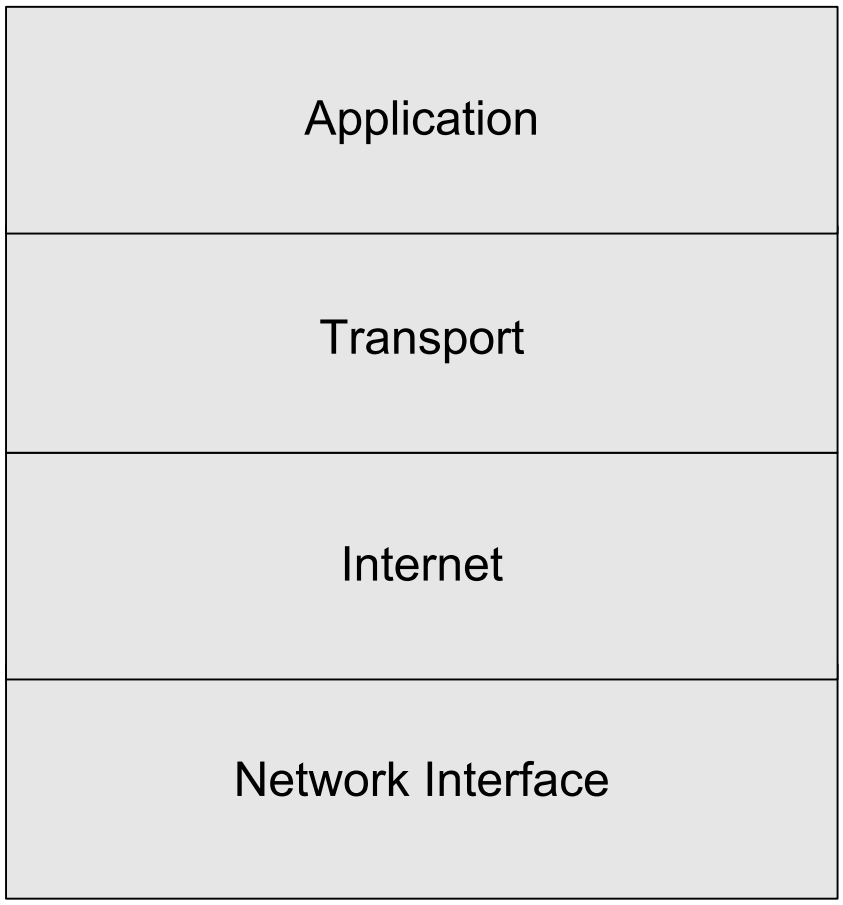


Figure 1-2: TCP/IP Layer Model

APPENDIX B

3.0 Functional Design Characteristics

This section describes the functional requirements of this interface.

3.1 Functional Design Characteristics

3.1.1 Network Interface Layer

The network interface layer handles the hardware details or the physical interfacing to the transmission medium (e.g., cable, radio link). It provides the mechanical, electrical, functional, and procedural methods necessary to activate, maintain, and deactivate physical connections for data links.

The following standards are allowable physical interface implementations in the CAR/SAM regions are described in the following paragraphs.

3.1.1.1 TIA/EIA-232-E/F

The TIA/EIA-232-E/F should be implemented according to TIA/EIA-232-E/F documents.

3.1.1.2 TIA/EIA-530-A

The TIA/EIA-530-A should be implemented according to TIA/EIA-530-A document.

3.1.1.3 V.35

The V.35 should be implemented according to ITU-T V.35 document.

3.1.1.4 Ethernet

Transmission of IPv4 datagrams over Ethernet networks should be in accordance with RFC 894. IPv6 based networks should conform to RFC-2464.

3.1.1.5 Frame Relay (FR)

Transmission of IPv4 datagrams over Frame Relay should be done in accordance with RFC-2427.
Transmission of IPv6 datagrams over Frame Relay should be done in accordance with RFC-2590.

3.1.2 Internet Layer

The Internet layer specifies the protocols that provide services corresponding to the internet layer. The protocol used in this layer for the CAR/SAM shall be Internet Protocol (IP). IP is designed for use in interconnected packet-switched computer communication networks and provides addressing and fragmentation services.

3.1.2.1 Internet Protocol

Two versions of this protocol shall be allowable for the CAR/SAM – the commonly available IPv4, and the upcoming IPv6 .

IPv4 implementations shall be in accordance with RFC-791.
IPv6 implementations shall be in accordance with RFC-2460.

APPENDIX B

3.1.2.2 Network addressing

Network addressing should be in accordance with RFC-796 for IPv4 implementations. IPv6 implementations in the CAR/SAM should be in accordance with RFC-2373.

3.1.2.3 Subnet extensions

Subnet extensions to the addressing architecture for IPv4 networks should be in accordance with RFC-950.

3.1.2.4 Tunneling over IPv4

Tunneling of datagrams (e.g., CLNP, ES-IS) over IPv4 should be done in accordance with RFC-2784.

3.1.2.5 Tunneling over IPv6

Tunneling of datagrams (e.g., CLNP, ES-IS) over IPv6 should be done in accordance with RFC-2473.

3.1.3 Transport Layer

The transport layer provides communication session management between host computers. It defines the level of service and status of the connection used when transporting data. Transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis.

3.1.3.1 Transmission Control Protocol (TCP)

Implementations of TCP shall be in accordance with RFC-793 and RFC-3168.

APPENDIX B

APPENDIX A - ACRONYMS

A.0 Acronyms

This appendix defines the acronyms used in this document.

A/G	AIR-GROUND
AAC	Aeronautical Administrative Control
ABM	Asynchronous Balanced Mode
AIDC	ATS Interfacility Data Communications
AMHS	ATS Message Handling System
AOC	Aeronautical Operational Control
APC	Aeronautical Passenger Communication
APRLs	ATN Protocol Requirement Lists
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Service
ATSC	Air Traffic Service Control
CLNP	Connectionless Network Protocol
CLNS	Connection-Less Network Service
CPDLC	Controller Pilot Data Link Communications
DCE	Data Circuit-terminating Equipment
DM	Disconnected Mode
DTE	Data Terminal Equipment
E/R	Error Report
EIA	Electrical Industry Association
ERD	End Routing Domain
ES	End System
FIB	Forwarding Information Base
FSM	Finite State Machine
G-G(G/G)	Ground-Ground
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
IDRP	Inter Domain Routing Protocol
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Sector

APPENDIX B

LAPB	Link Access Procedure Balanced
NET	Network Entity Title
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PIB	Policy Information Base
PICS	Protocol Implementation Compliance Statement
PSDN	Public Switched Data Network
PSN	Packet Switched Network
PVC	Permanent Virtual Circuit
QOS	Quality of Service
RD	Routing Domain
RDC	Routing Domain Confederation
RIB	Routing Information Base
SARPs	Standards and Recommended Practices
SNDCF	Sub Network Dependent Convergence Functions
SNPA	Sub Network Point of Attachment
SVC	Switched Virtual Circuit
TBD	to be Determined
TBR	to be Reviewed

APPENDIX C

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Fifth Meeting of the CAR/SAM ATN Task Force (CAR/SAM/ATF3)
Mexico City, Mexico 12-13 June 2009

CAR/SAM AMHS IP ROUTING POLICY (AMHS GROUND-TO-GROUND VERSION)

VERSION 2.00
(THIRD DRAFT)

WORKING PAPER

(PRESENTED BY THE UNITED STATES OF AMERICA)

Summary

This paper presents a set of recommended routing policies for the Caribbean/South America (CAR/SAM) Region Aeronautical Telecommunications Network (ATN) Message Handling system (AMHS) service using the Internet Protocol that is based on MEVA and REDDIG networks as well as dedicated circuits.

APPENDIX C

Executive Summary

The CAR/SAM Region has agreed to use IPv4 as the underlying communication infrastructure for AMHS instead of the ATN ICS. In order to route AMHS messages between States and Organizations in the Region, BGP-4 has been selected as the routing protocol. This document presents the definition of routing policies that should be enforced between BGP-4 routers within the Region.

APPENDIX C

Document Control Log

Edition	Date	Comments	Section/pages affected
0.1	23 Mar. 2007	First Draft	All
.02	28 Jun. 2008	Second Draft	Add Document Control Log
2.00	13June, 2009	Third Draft	Ultilize IPv4 and MEVA/REDDIG/Dedicated circuits

APPENDIX C

APPENDIX C

1 Introduction

The CAR/SAM Aeronautical Telecommunications Network (ATN) Task Force is developing its plans for implementing ATN applications throughout the Region. The plans are being described in a set of documents. This document, as a part of the set, describes the network routing protocols and policies that define the Regional network routing.

1.1 Objective

This document is meant to describe the Regional routing protocols and policies that are to be used for the use of the ATN AMHS. Supporting the decisions made by the Task Force, this document focuses on the specification of routing protocols and policies based on the use of the IPS-based networks for exchanging ATN AMHS messages.

1.2 Scope

This document is limited to describing the IPS routing protocols and policies to be used between States and Organizations (inter-domain) within the Region.

1.3 References

[1]	ICAO Doc 9705-AN/956	Manual of Technical Provisions for the ATN
[2]	TBD	Proposed Draft of the CAR/SAM Regional AMHS Transition Plan
[3]	RFC 4271	BGP-4 Specification
[4]	RFC 4272	BGP Security Vulnerabilities Analysis
[5]	RFC 4360	BGP Extended Communities Attribute
[6]	RFC 4384	BGP Communities for Data Collection
[7]	RFC 4451	BGP MULTI_EXIT_DISC (MED) Considerations
[8]	RFC 4456	BGP Route Reflection: An Alternative for Full Mesh Internal BGP (IBGP)
[9]	RFC 4486	Sub codes for BGP Cease Notification Message
[10]	RFC 4724	Graceful Restart Mechanism for BGP
[11]	RFC 4760	Multiprotocol Extensions for BGP-4
[12]	RFC 4781	Graceful Restart Mechanism for BGP with MPLS

1.4 Terms Used

Routing Domain	–	A collection of systems that are administered by a single administrative authority that is regulated by a particular set of administrative guidelines. Routing domains are also called autonomous systems.
Intra-domain routing	–	The routing of packets within a single routing domain. Intra-domain routing is based on a level of trust between systems operating within the domain.

Inter-domain routing	–	The routing of packet between routing domains. Inter-domain routing is based on mutual miss-trust in the reception of routing information from other domains.
Autonomous System	–	Another term used within the Internet community for Routing Domain

1.5 Acronyms

ATN	–	Aeronautical Telecommunications Network
AMHS	–	ATN Message Handling System
CLNP	–	OSI Connectionless Network Protocol
IDRP	–	OSI Inter-Domain Routing Protocol
ICS	–	ATN Internet Communication Service
ES	–	End System
IS	–	Intermediate System
NSAP	–	Network Service Access Point
BIS	–	Border Intermediate System
BBIS	–	Backbone Border Intermediate System
BG	–	Border Gateway
BGP	–	Border Gateway Protocol
RFC	–	Internet Engineering Task Force Request For Comment
IPS	–	Internet Protocol System
PDU	–	Protocol Data Unit
MPLS	–	Multiprotocol Labeling System

1.6 Overview of IPS Specification Issues

The following subsections present issues that affect the completion of the routing policy document and/or in operating the IPS-based AMHS network.

1.6.1 BGP-4 Specification

The BGP-4 RFC [3] presents the overall definition of the protocol and its operation. However as in any complex protocol specification, there are options and methods of operation that require users of the protocol to make a more detailed selection. Since BGP-4 is designed to use IPv4, a separate specification [11] is also needed to specify BGP-4 over IPv6. At the present time, there is no BGP-4 specification for the Region. This makes the development of policy difficult.

Examples of issues to be decided are:

- disposition of routing tables (last paragraph of the overview section),
- value and calculation of the HOLD timer,
- use of AS-PATH parameter, and
- aggregation requirements.

APPENDIX C

The set of documents describing BGP-4 includes several that define optional/extended parameters (see [5] and [6]). The use of optional parameters needs to be carefully defined.

The set of documents describing BGP-4 includes several that define optional/extended mechanisms (see [7], [8], [10] and [12]). The use of optional mechanisms needs to be carefully defined.

The current approach is based on MEVA and REDDIG network with dedicated circuits.

1.6.2 Use of TCP

BGP-4 uses TCP connections for the exchange of information. As a part of the use of BGP-4, a specification of TCP parameters and timers for use in the region is needed.

This can be achieved during the test procedure between associated states.

1.6.3 Use of TCP MD5

For the authentication of BGP-4 peers, the TCP MD5 options are mandatory. However, this requires the generation, distribution, and management of the certificates. Both the technical and administrative aspects of the use of MD5 need to be defined.

1.6.4 Autonomous System Number Assignment

In order to operate as a BGP-4 router, each router must be assigned a unique AS number. At the present time, these numbers are assigned by IANA.

The region has already proposed and in the process to finalize IPv4 addressing scheme. This is a closed and private network that is based on MEVA and REDDIG. Therefore, coordination with IANA is not necessary.

1.6.5 IPv6 Address Architecture

A central feature missing between the use of the ATN ICS and the IPS is the definition of a comprehensive IPv6 addressing architecture. In the case of the ATN ICS, the NSAP is divided into a hierarchy. The hierarchy is based on the “owner” of each part of the address space and maps to the hierarchical nature of routing domains. The use of the NSAP address hierarchy by IDRP enables a considerable reduction in routing information dissemination.

An IPv6 address structure is needed that enables the efficient aggregation of routes based on a global or regional basis.

IPV6 is not considered in the immediate future per the regional planning. IPv4 addressing schemes has been proposed and in the process to be adopted by the region.

1.6.6 Security

The developers of BGP-4 understand that there are security issues relating to route dissemination (see [3]). The selection of options and/or procedures has not been decided.

APPENDIX C

The region needs to review the security requirement such as authentication or verifying network (establishing Virtual Private Network or using dedicated circuits/channels)

2 Background

The ATN AMHS as defined in Sub-Volume 3 of [1] is based upon the use of the ATN ICS and utilizes the OSI transport protocol, CLNP, and IDRP for the exchange of messages across the network. There has been considerable debate on the use of the IPS as a replacement for the ATN ICS protocols and this Region has agreed to use the IPS within the Region and with States in other Regions that support these protocols.

One of the problems when discussing the routing architecture for the ATN is that it uses the terminology from the OSI Reference Model where the terminology from the IPS is somewhat different. This section describes and contrasts the two terminologies while explaining the routing architecture for the Region.

2.1 Routing Domain Fundamentals

2.1.1 Domains

Using the terminology of the ICAO/ATN, the ATN consists of a set of End Systems (ESs) and a set of Intermediate Systems (ISs). End systems are typically the computers that contain the applications and are not involved with routing packets to other systems. Intermediate systems are typically routers.

The ESs and ISs are organized into *Routing Domains*. Routing Domains are used to define sets of systems (that typically operate together) into clusters. These clusters have two major properties:

- they are controlled by a single organization, and
- a significant amount of the traffic is internal to the cluster.

The single most important characteristic is that they are controlled by a single organization. This characteristic is manifested in technical terms by mutual trust between all routers in a routing domain. Routing protocols are based on the fact that the information exchanged between *intra-domain* (within a domain) routers can be trusted. No special reliability or trust is required to accept information about advertised routes.

The second characteristic, most traffic is internal to a routing domain, is more an artifact of proper network engineering. In the ATN, routing domains are established through the NSAP addressing conventions established for the ATN in Doc 9705, Sub-Volume 5. All systems with NSAP addresses defined with the same address prefix are by definition in the same routing domain. Within the IPS, routing domains may be established by IPv6 address conventions. The definition of the IPv6 address architecture for the CAR/SAM Region may have significant impacts on the definition of the appropriate routing domain structure.

2.1.2 Intra-Domain Routing

Intra-domain routing is the routing of PDUs from the source to destination where both are in the same domain. Intra-domain routing implies one or more ISs capable of routing PDUs across the domain. Examples of intra-domain routing would be CLNP-capable routers exchanging PDUs between two Local Area Networks.

APPENDIX C

2.1.3 Inter-Domain Routing

The central definition of routing in the ATN is concerned with inter-domain routing. This is a particularly difficult problem since by the very nature of inter-domain routing; the information received cannot be fully trusted.

Inter-domain routing is based upon the mutual distrust of the received routing information. First, reliability mechanisms must be build-in to ensure the reliable transfer of the information. Second, the received information must be filtered to ensure that it meets the suitability constraints of the received system (in other words, it can be believed.)

After receiving routing information, the inter-domain router must build routing tables based upon its internal policy about routing its data.

2.1.4 Types of Routing Domains

There are two basic types of routing domains: end routing domains, and transit routing domains. An end routing domain routes PDUs to and from end-systems within its routing domain. Figure 1 shows an end routing domain.

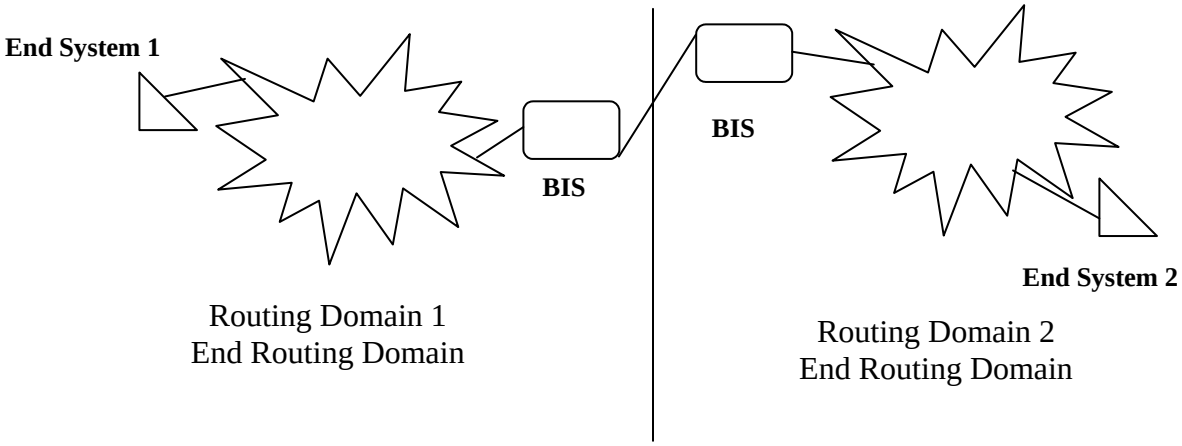


Figure 1 – End Routing Domains

A transit routing domain routes PDUs between two or more routing domains, and may as an option also act as an end routing domain. An example of a transit domain is where a set of backbone routers is configured in their own routing domain with all of the end systems in end routing domains attached to the backbone. Figure 2 shows Routing Domain 2 as a transit routing domain.

APPENDIX C

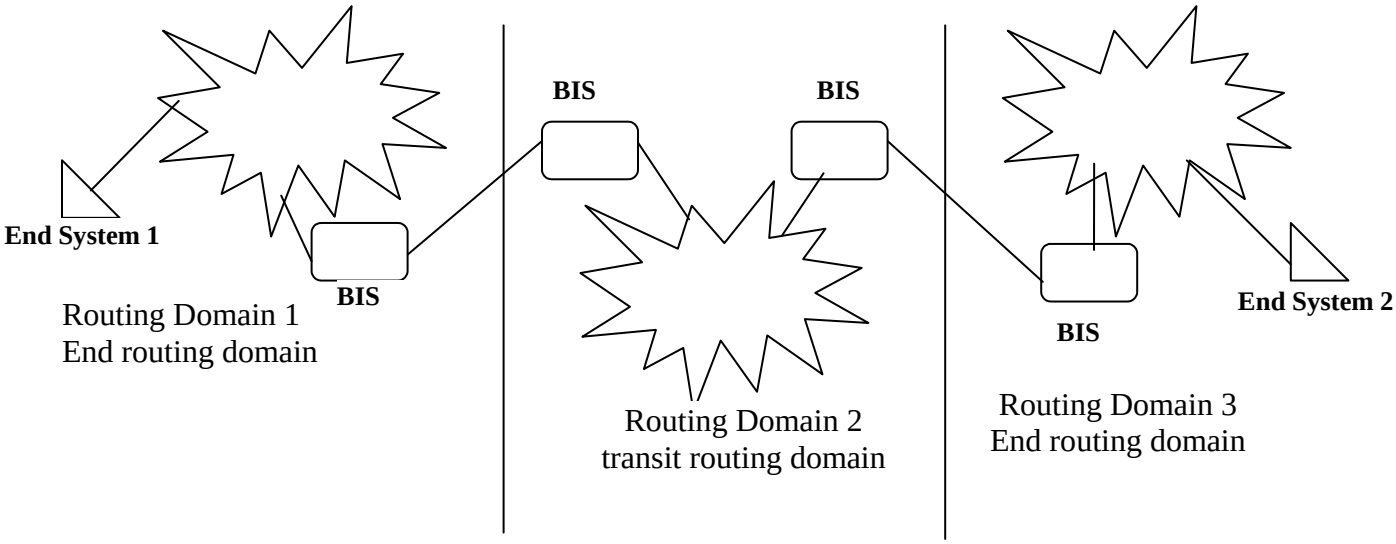


Figure 2 – Transit Routing Domains

2.1.5 Routing Domain Definition Requirements

For each routing domain that is accessible in the Region, there must be at least one inter-domain router. (In ATN terms, there must be at least one Boundary Intermediate System (BIS) for each routing domain supporting AMHS.)

2.1.6 IPS Autonomous Systems and Routing

As mentioned earlier, the terminology between ATN/OSI and the IPS is somewhat different. In the context of the IPS documentation, the term Autonomous System (AS) is introduced to define a network or set of networks that managed by a single organization. The use of AS is needed since there is not the same concept as "routing domain" in the IPS architecture.

The addressing scheme for IPv6 (and IPv4) does not include the concept of routing domains. Rather any defined address prefix length can be used for routing without regards to "domains". The AS terminology is a way to describe routing domains through the use of network(s) management. For the purposes of describing routing using IPS, an AS can be considered equivalent to an ATN/OSI routing domain.

2.2 Router Fundamentals

All routers and routing protocols discussed within this document are ICAO Doc. 9705 Boundary Intermediate Systems (BISs). Using the IPS terminology, all routers discussed within this document are "Border Gateway (BG)" routers that communicate between Autonomous Systems.

2.2.1 BIS and Border Gateway Systems

There are two primary types of BISs (or BGs) employed within the Region:

- Backbone BISs/BGs (BBISs/BGs), and
- End BISs/BGs (EBISs/EBGs)

2.2.1.1 Backbone BIS/BG

A BBIS/BBG is a router that primarily routes PDUs between routing domains or ASs. These routers are typically higher performance routers that aid in the efficient flow of data between domains/ASs. BBIS/BBG may have End-Systems connected to them, but they are often limited to router-to-router connections.

Within the context of the CAR/SAM Region, BBISs/BGs can be further subdivided into Regional BBIS/BGs and Inter-Regional BBISs/BGs. Regional BBISs/BGs are backbone routers that only connect to routers within the Region. Inter-regional Backbone BBIS/BGs are those backbone routers that also connect to BBISs in other Regions.

Note 1: A single, high-performance router may act as both a Regional BBIS and an Inter-Regional BBIS based upon meeting the requirements for performance and reliability.

Note 2: For completeness of the routing architecture, it must be mentioned that the router out-side of the Region to which Inter-Regional Backbone BISs attach are, in fact, Inter-Regional Backbone BISs in the other Region.
Note 3: The interconnection of backbone BISs typically require higher capacity communication lines based on the consolidation of traffic through those backbone routers. Even thought the architecture takes into account existing AFTN infrastructure facilities, the need to upgrade the communication facilities as traffic throughout the backbone increases may be necessary.

Note 4: It is possible for some States to provide transit routing from its routing domain to the routing domains of other States using BISs that are not backbone routers. For the purposes of this routing architecture, it is not possible to distinguish between these transit routing domain routers and BBISs.

Note 5: Due to the restrictions of the ICAO SARPs, Inter-Regional BBISs may be limited to ATN-compliant routers. Bi-lateral agreements between States providing Inter-Regional routing may allow for routers using the IPS.

2.2.1.2 End BIS

End BISs/BGs are connected to one or more BBISs/BBGs and provide routing services to a single routing domain/AS. Further End BISs do not act as a transit router for passing PDUs between other routing domains/AS.

2.3 CAR/SAM AMHS Ground-to-Ground Routing Architecture

The CAR/SAM AMHS routing architecture is to the largest degree possible independent of the protocol family (ATN/OSI or IPS) or specific routing protocols. The CAR/SAM routing architecture is based upon several concepts:

APPENDIX C

1. From the IPv6 addressing specification, “routing-domains” are defined as specific address prefix lengths.
2. Based on the definition of “routing-domain” prefix definitions, each routing domain can be considered an Autonomous System (AS).
3. States will make their own implementation and transition decisions.

The routing architecture can be divided into several distinct parts:

- the definition of the backbone routing structure for passing information between routing domains within the Region;
- the definition of the routing structure between routing domains not on the backbone;
- the definition of the routing structure for use in end-routing domains; and
- the definition of the routing structure for passing information from this Region to other Regions.

The first component is the definition of the backbone routing structure that supports the exchange of data within the Region. This part defines the interconnection of the major communication facilities in the Region and how they cooperate to link all of the systems in the Region.

The second component is the definition of the structure that allows end routing domains to exchange data across the backbone to anther end routing domain. This part defines how the end routing domains connect through the backbone.

The third component defines the routing structure that is used within an end routing domain. This part defines how the individual routing domains may be used to pass data.

The fourth part is needed to define how data will be routed between the systems within the Region and those systems outside the Region. More importantly, the structure describes how all global ATN systems are accessible from systems in the Region.

2.3.1 CAR/SAM Backbone

The definition of a Regional Backbone is based upon the efficiencies that may be realized by concentrating AMHS traffic at major communication centers and using the economy of scale in passing this information between major communication centers.

The rationale for defining Regional Backbone sites is based upon existing major AFTN center sites and on the flow of both AFTN traffic and possible future AMHS/ATN traffic.

The CAR/SAM Region is comprised of a large number of States spread over a wide geographic area. Within the Region, there are existing main AFTN communication centers that can be used to simplify the definition of the backbone architecture.

The architecture and communication requirements define a routing plan that incorporates alternate routing and communication paths so that no single router or communication failure can isolate major parts of the Region.

Based on the previous paragraphs, the CAR/SAM Backbone network will consist of at lease on BBIS router at each of the backbone sites identified in Table A-1.

The States implementing a backbone router site needs to select is router(s) based on the expected availability, reliability, capacity, and alternate communication path requirements.

2.3.2 Inter-Regional Backbone

The second component of the CAR/SAM Routing architecture is the definition and potential location of Inter-Regional Backbone Routers. The manner in which this architecture was developed was to ensure that the use of the existing communication infrastructure is possible to the greatest degree. The use of the existing communication infrastructure should reduce the overall cost of transitioning to the AMHS.

To re-state from the previous section, the Inter-Regional BBISs provide communication from routers within the CAR/SAM Region to routers in other regions. These Inter-Regional BBISs provide vital communications across regions and therefore need to have redundant communication paths and high availability.

The location of Inter-Regional BBISs is TBD.

Note: These routers may need to be ATN-compliant.

2.3.3 End BISs

It is assumed that naming and addressing (and routing domain definition) will be done on a Regional basis. Further that for areas within the Region that may utilize an End BIS service more than one State, the naming structure will be based on the Regional IPv6 addressing plan as defined.

2.4 AMHS IPS-Based Ground-to-Ground Routing

The Region has already made the decision to provide ATN AMHS services over an appropriately defined TCP/IPv6 communication infrastructure. The following sections describe the implementation of the Regional routing architecture within the scope of IPv6 routing.

2.4.1 Internet Protocol Suite Routing Protocols

Within the scope of the routing of IPv6 traffic there are defined several different protocols. For the purposes of intra-domain routing typical protocols are RIPv2 and OSPF. For the purposes of inter-domain routing, BGP-4 is the most prevalent.

For that reason and its close relationship with the ATN IDRP, BGP-4 is selected as the Regional Inter-domain protocol.

3 BGP-4

The **Border Gateway Protocol (BGP)** is the routing protocol used to exchange routing information across the Internet. It makes it possible for ISPs to connect to each other and for end-users to connect to more than one ISP. **BGP** is the only protocol that is designed to deal with a network of the Internet's size, and the only protocol that can deal well with having multiple connections to unrelated routing domains.

APPENDIX C

3.1 BGP-4 Requirements

In order to use BGP-4 for routing within the Region, each BGP-4 router must meet the following minimum requirements.
Each routing-domain/AS must obtain an AS number.

Note: The method of obtaining an AS number is within the scope of the IPv6 Address document.

Each BGP-4 router must have an appropriate MD-5 certificate/password assigned and managed.

Note: The procedures for generating, managing, distributing MD-5 certificates are TBD.

3.2 Policy Based Routing

3.2.1 Types of Policy

The BGP-4 decision process (and thus AMHS routing policy) is conditioned by three types of policy concerns.

- *Route Aggregation* policies permit BGP-4 routers to reduce the amount of routing information propagated.

- *Route Preference* policies determine which routes will be installed in the Forwarding Information Base. Route preference policies thus determine which path a router will select to forward IPv6 pdus on.

- *Route Distribution* policies determine which routes a BGP-4 router will advertise to other BGP-4 routers. Route distribution policies are a key aspect of a routing-domain's/AS's transit policy in that they determine which routes will be permitted in a domain. A BGP-4 router will not propagate a route, which it does not wish to support. By selective advertisement of routing information BGP-4 routers control the use of their own resources since other routers cannot choose a route they do not know about.

4 General Framework for AMHS BGP-4 Routing Policy

4.1 Routing Policy Goal for BGP-4 routers

The AMHS CAR/SAM Regional infrastructure must support a consistent set of routing policies to provide paths to AMHS systems at an inter-regional, intra-regional and local level without an inordinate number of routing protocol updates. Accordingly, the detailed policy requirements and recommendations specified in section 4 are derived from the following general routing policy goal:

- **CAR/SAM Regional BGP-4 routers will provide global shortest path connectivity with a minimal exchange of routing information.**

- **CAR/SAM Regional BGP-4 routers will not exchange any routing information for any IPv6 address not defined as an "ICAO State or Organization" address. (No connectivity to global internet routers or hosts.)**

- **CAR/SAM Regional BGP-4 routers will not connect to any router not owned or operated by a State or Organization. (No connectivity to global internet routers or hosts.)**

Note: Providing paths/routes for inter-regional AMHS connectivity may require additional routing requirements based on the need to relay the AMHS message through an MTA that can provide connectivity between ATN/OSI (ATN router-based) infrastructures and the CAR/SAM IPS infrastructure.

4.2 Network Organization for Routing to Ground Systems

As presented in earlier sections, the AMHS ground infrastructure may be partitioned into various levels of organization. Routing domains at the highest level are associated with an ICAO region. The CAR/SAM IPv6 Addressing Plan should provide an IPv6 address structure that partitions the address space to include NLRI prefixes that vary according to the level of organization. Within the CAR/SAM Region, routing domains are next associated with a particular state or organization. Note that the regional addressing plan should specify a field within the IPv6 address that can be uniquely assigned to the state or organization. Finally, within a particular state or organization there may be multiple local routing domains (which may or may not be visible outside of the particular state or organization).

Note: For the purposes of the following paragraphs, an AMHS ground router is a router supporting IPv6 routing via BGP-4.

Within this framework AMHS ground routers may be characterized and their policy requirements specified according to the type of connectivity they have to adjacent AMHS ground routers. AMHS routers connecting to adjacent routers in another region are said to have “inter-regional” connectivity [Note: these most likely will be actual ATN/OSI ground routers]. AMHS routers connecting to adjacent routers in another state or organization within the CAR/SAM Region are said to have “intra-regional” connectivity. AMHS routers connecting to adjacent routers within a particular state or organization are said to have “local” connectivity, i.e. intra-state or intra-organizational connectivity.

4.3 Policy for BGP-4 Routes to AMHS Systems

The policy requirements for BGP-4 routers in the CAR/SAM Region for routes to AMHS systems are specified in this section. The following sub-sections specify the policies according to the classification:

1. the general policy for routes to ground systems; the policy for inter-regional routes;

2. the policy for intra-regional routes; and

3. the policy for local routes.

***Note 1**. – This section specifies routing policy requirements for backbone routers in the CAR/SAM region. A backbone router is a BGP-4 router which has been designated by the operating state/organization to provide an appropriate level of performance and support the routing policies for inter-regional and intra-regional connectivity, and whose operation as a backbone router has been approved by the ICAO regional office as agreed-to by all other member states/organizations. This section also contains a number of recommended policies non-backbone routers.*

APPENDIX C

***Note 2**. – This document and companion documents specify requirements for AMHS ground routers in the "Caribbean and South America (CAR/SAM) region"; however, from the perspective of the AMHS Ipv6 Addressing Plan, there is/may not be a single "CAR/SAM region" but rather there is a distinct Caribbean region and a distinct South American region each with a unique region identifier.*

4.3.1 General Policy

a) If a backbone router receives multiple routes to an aggregate or specific destination, the route with the shortest path ([i.e., shortest list of AS)] shall be selected.

b) All BGP-4 routers in the Region shall authenticate the identity of peer ATN routers.

***Note**. – Authentication may be accomplished via the mandatory MD-5 option.*

4.3.2 Policy for Inter-Regional Aggregate Routes To Ground Systems

Inter-Regional route aggregation is only possible where a bi-lateral agreement exists between the two States to operate BGP-4 routers.

4.3.3 Policy for Intra-Regional Aggregate Routes to Ground Systems

Intra-regional route aggregation permits advertisement of a single aggregate route which identifies all systems in a particular State or Organization of an ICAO region. Aggregation at an intra-regional level refers to aggregating NLRI fields in the IPv6 address prefix up through the complete [TBD] field.

***Note**: The IPv6 addressing plan needs to develop the appropriate NLRI prefix hierarchy.*

4.3.3.1 Intra-Regional Route Aggregation Policies

a) Backbone routers with intra-regional connectivity shall be configured with aggregate routes to AMHS system at an intra-regional level.

4.3.3.2 Intra-Regional Route Preference Policies

Backbone routers with intra-regional connectivity shall accept intra-regional aggregate routes to AMHS systems from adjacent ATN routers.

Recommendation. Backbone routers with intra-regional connectivity should only accept inter-regional or intra-regional aggregate routes on these connections.

4.3.3.3 Intra-Regional Route Distribution Policies

b) Backbone routers with intra-regional connectivity shall distribute intra-regional aggregate routes to adjacent AMHS BGP-4 routers.

c) Routers with local connectivity shall distribute intra-regional aggregate routes to adjacent AMHS BGP-4 routers.

Recommendation. Non-Backbone routers with local connectivity should distribute intra-regional aggregate routes to adjacent AMHS BGP-4 routers.

APPENDIX C

4.3.4 Policy for Aggregate Routes to Ground Systems for Distinct Routing Domains within a State/ Organization

Distinct Routing Domain-level aggregation permits advertisement of a single aggregate route which identifies all systems in a specific routing domain of a particular State or Organization of an ICAO region. Aggregation at this level refers to aggregating NLRI fields to an agreed IPv6 address prefix [TBD]. AMHS BGP-4 routers connecting to adjacent routers within a particular state or organization, i.e., with intra-state or intra-organizational connectivity, are said to have "local" connectivity.

4.3.4.1 Distinct Routing Domain Route Aggregation Policies

Recommendation. AMHS BGP-4 routers serving individual routing domains should be configured with aggregate routes to all other AMHS systems.

4.3.4.2 Distinct Routing Domain Route Preference Policies

Recommendation. AMHS routers with local connectivity should accept state/organizational-level aggregate routes from adjacent AMHS BGP-4 routers within the same state or organization.

4.3.4.3 Distinct Routing Domain Route Distribution Policies

Recommendation. AMHS BGP-4 routers with local connectivity should distribute state/organizational-level aggregate routes to AMHS ground systems only to adjacent AMHS BGP-4 routers within the same state or organization.

4.3.4.4 Local State/Organizational Routing Policies

Individual states/organizations may have additional routing policies consistent with the above policies for routes to ground systems. Such policies may include various local preferences or Quality of Service based routing, for example, routing based on line error rates, expense, delay, capacity, and priority.

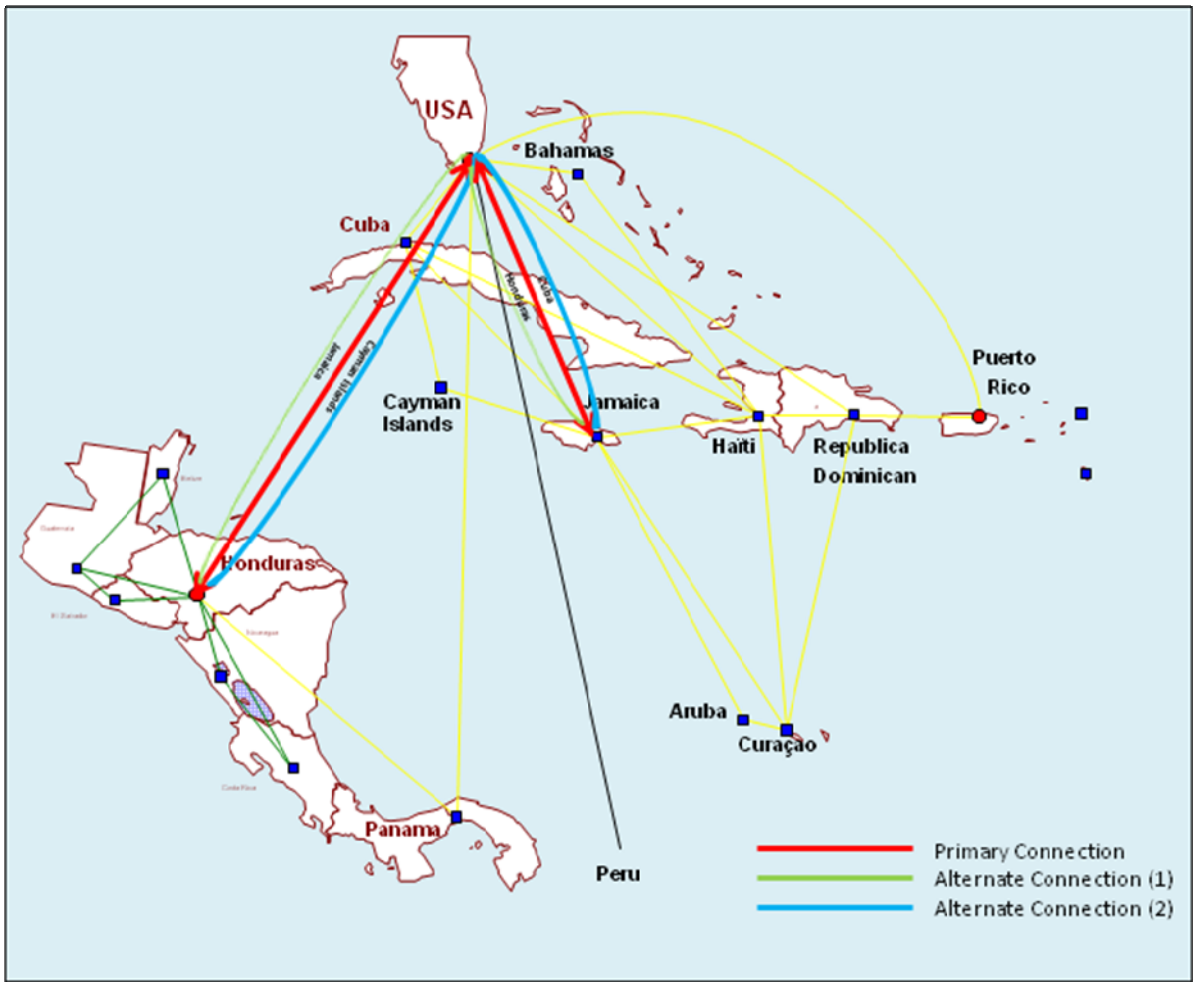
APPENDIX C

Proposed AMHS Routing

Major Backbones in the region

Honduras-USA (Primary route)
Honduras-Jamaica-USA (Alternative Routing 1)
Honduras-Cayman Island-USA (Alternative routing 2)

Jamaica-USA (Primary routing)
Jamaica-Honduras-USA (Alternative routing 1)
Jamaica-Cuba-USA (Alternative routing 2)



APPENDIX C

Venezuela-USA (Primary routing)
Venezuela-Trinidad-USA (Alternative routing 1)
Venezuela-Peru-USA (Alternative routing 2)

Venezuela-Trinidad (Primary routing)
Venezuela-USA-Trinidad (Alternative routing 1)

Venezuela-Brazil (Primary routing)
Venezuela-Peru-Brazil (Alternative routing 1)
Venezuela-USA-Brazil (Alternative routing 2)

Venezuela-Peru (Primary routing)
Venezuela-Brazil-Peru (Alternative routing 1)
Venezuela-USA-Peru (Alternative routing 2)

Trinidad-USA (Primary routing)
Trinidad-Antigua-USA (Alternative routing 1)
Trinidad-Venezuela-USA (Alternative routing 2)

Colombia-Peru (Primary routing)
Colombia-Venezuela-Peru (Alternative routing 1)
Colombia-Ecuador-Peru (Alternative routing 2)

Peru-Brazil (Primary routing)
Peru-Venezuela-Brazil (Alternative routing 1)
Peru-USA-Brazil (Alternative routing 2)

Peru-Venezuela (Primary routing)
Peru-USA-Venezuela (Alternative routing 1)
Peru-Brazil-Venezuela (Alternative routing 2)

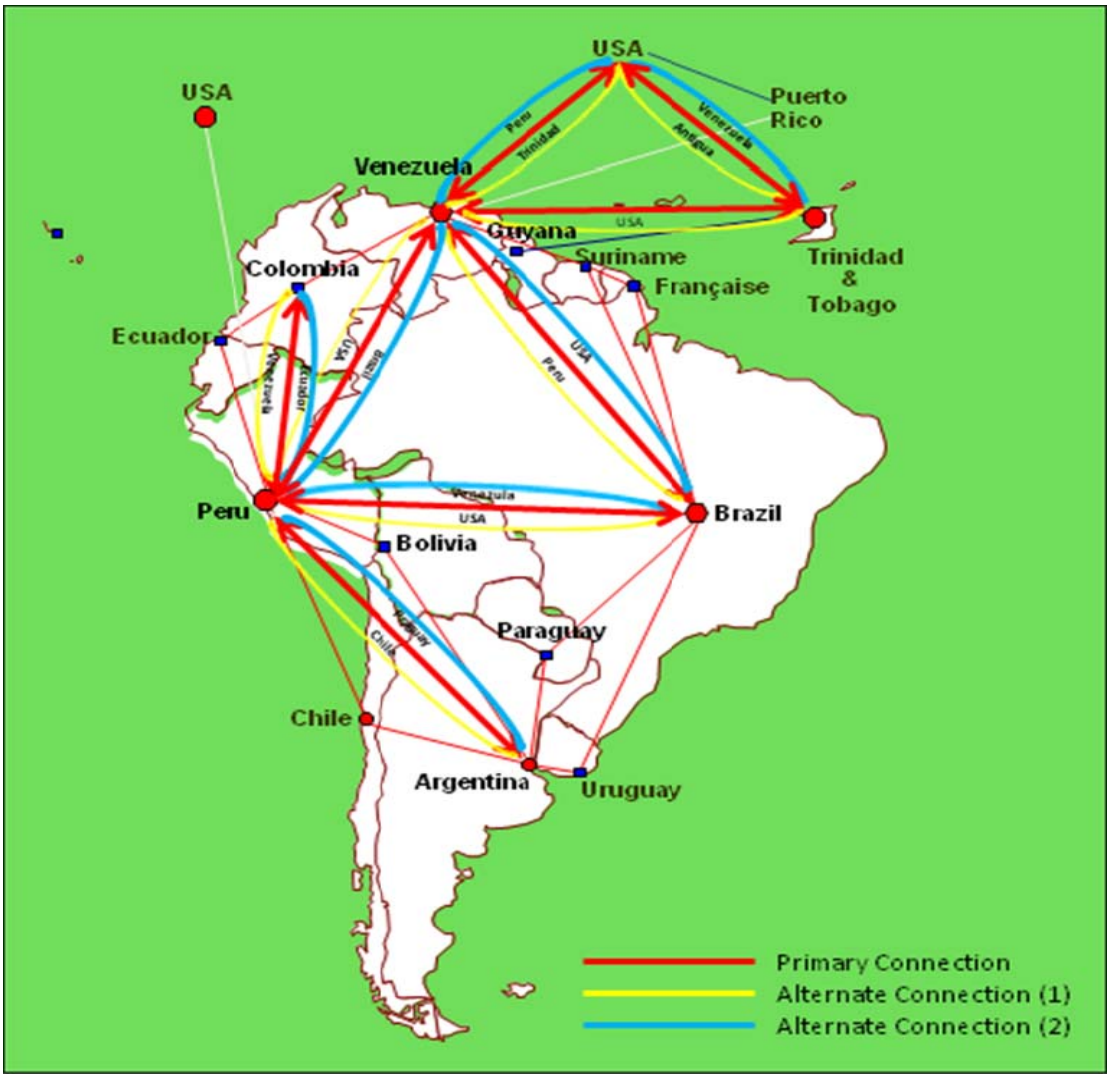
Argentina-Peru (Primary routing)
Argentina-Chile-Peru (Alternative routing 1)
Argentina-Paraguay-Peru (Alternative routing 2)

APPENDIX C

Brazil-Peru (Primary routing)

Brazil-USA-Peru (Alternative routing 1)

Brazil-Venezuela-Peru (Alternative routing 2)



APPENDIX C

Brazil-USA (Primary routing)

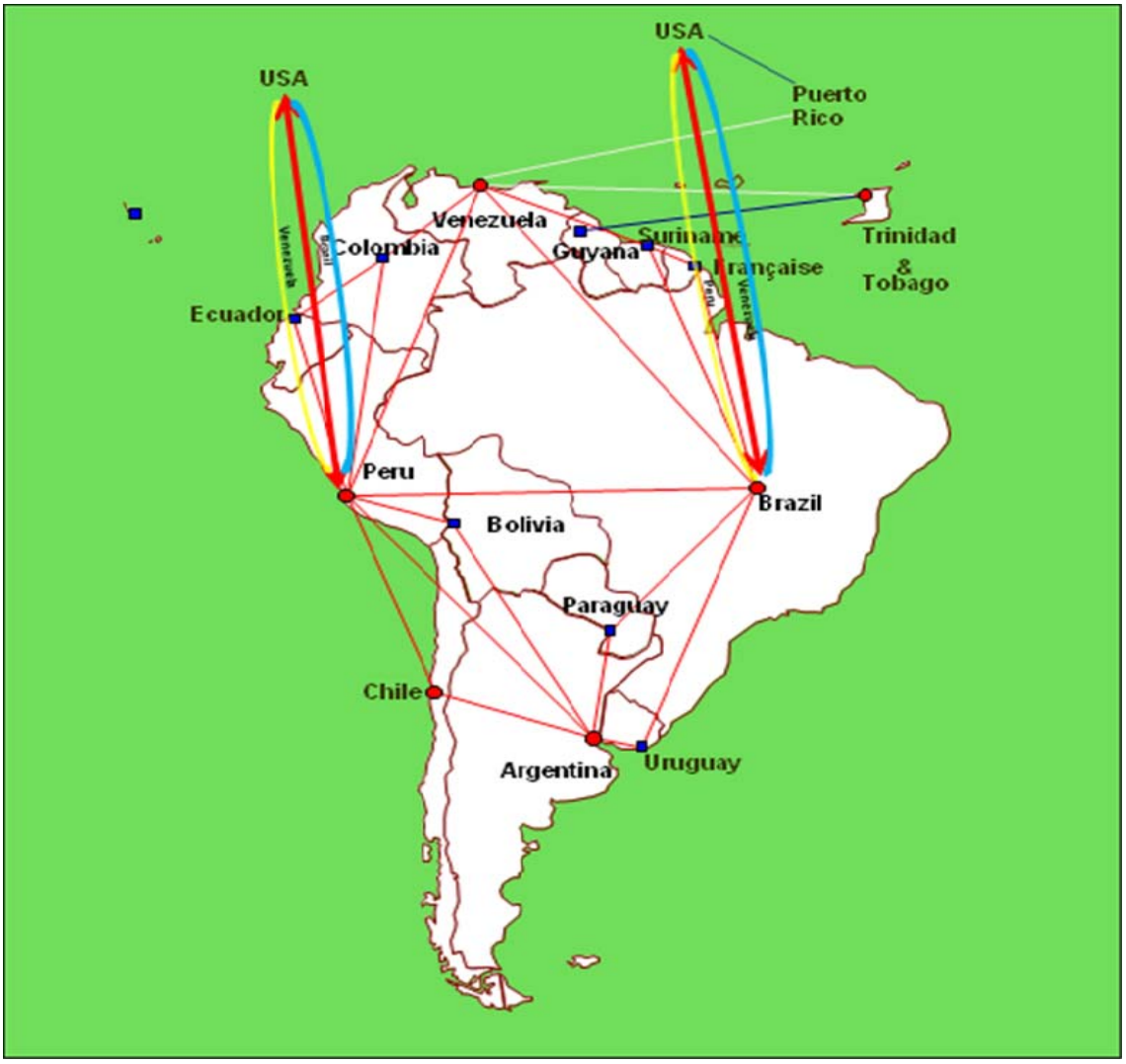
Brazil-Peru-USA (Alternative routing 1)

Brazil-Venezuela-USA (Alternative routing 2)

Peru-USA (Primary routing)

Peru-Venezuela-USA (Alternative routing 1)

Peru-Brazil-USA (Alternative routing 2)



APPENDIX D

International Civil Aviation Organization

THE FOURTH MEETING OF
AERONAUTICAL TELECOMMUNICATION NETWORK (ATN)
IMPLEMENTATION CO-ORDINATION GROUP OF APANPIRG (ATNICG/4)

Mexico 12 - 13 June 2009

Agenda Item 1: Review of the ATN CAR/SAM Planning/Implementation Activities

CAR/SAM AERONAUTICAL TELECOMMUNICATION NETWORK SECURITY GUIDANCE DOCUMENT

(Prepared and presented by FAA/USA)

SUMMARY

This paper provides The ATN Security Guidance Document for the CAR/SAM Region's guidance on the implementation of security for states and organizations operating in the region. It also includes **Contingency Plan Outline and Incident Response Plan Outline.**

DRAFT

First Edition

June 2009

TABLE OF CONTENTS

1. INTRODUCTION

This first draft Security Guidance Document for the CAR/SAM Region provides guidance on the implementation of security for states and organizations operating in the region.

1.1 Background

The fundamental objectives for system security of the ATN are to:

1. Protect ATN data from unauthorized disclosure, modification, or deletion, and
2. Protect ATN resources from unauthorized use and denial of service.

These objectives are achieved through the application of a set of high-level security services. The CAR/SAM Security Policy identifies the following services:

(1) Confidentiality. Ensures data is not disclosed to unauthorized entities.

(2) Data Integrity. Ensures data has not been altered or destroyed in an unauthorized manner.

(3) Authenticity. Ensures that the source of data or the identity of an entity is as claimed.

(4) Availability. Ensures resources, services, and data are accessible and usable on demand or in a timely, reliable manner by an authorized entity.

(5) Accountability. Enables activities to be traced to users and processes that may then be held responsible for those actions.

These security services are in turn realized by the implementation of a comprehensive set of management, operational, and technical controls. Controls may be organized into the following control classes:

Management controls are safeguards or countermeasures that focus on the management of risk and the management of system security.

Operational controls are safeguards or countermeasures for a system that are primarily implemented and executed by people.

Technical controls are safeguards or countermeasures for a system that are primarily implemented and executed by the system through mechanisms contained in the components of the system.

Figure 1.1 depicts the relationship between Security Objectives, Services, and Controls.

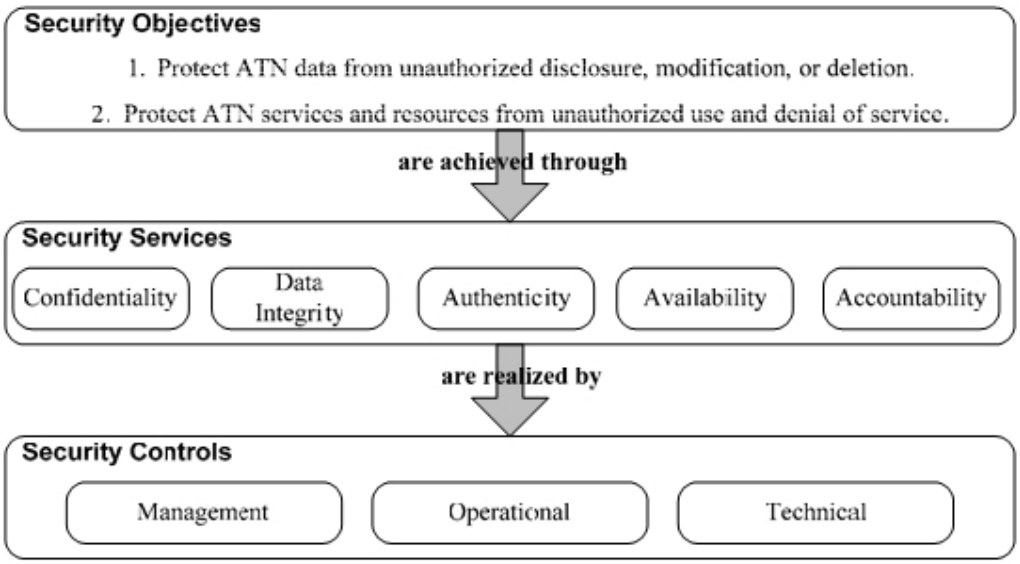


Figure 1-1. Security Objectives, Services, and Controls

1.2 Document Organization

In addition to this introduction, this document contains 4 major sections.

Section 2 provides a description of the 17 control families in the three Management, Operational, and Technical control classes. This section also provides a mapping from the high-level services to the control families.

Section 3 provides guidance on control families in the Management class. This section describes best practices for the management organization in an entity participating in the ATN.

Section 4 provides guidance on control families in the Operational control class. It describes procedures which constitute an effective security operation.

Section 5 provides guidance on control families in the Technical control class. Section 5 describes how technical controls are applied to various components of an ATN system. It gives specific examples of controls applied to each component.

2. SECURITY CONTROL FAMILIES

2.1 Description of Control Families

Access Control (AC) is the capability of the system to limit access to authorized users, processes acting on behalf of authorized users, and devices (including other systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT) ensures that operational personnel are aware of the security risks associated with their activities and the security policies which apply to their systems, and ensures that personnel are adequately trained to carry out their duties and responsibilities.

Audit and Accountability (AU) is the capability of the system to generate audit records that may indicate unauthorized or inappropriate system activity and that may be used to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA) ensures that the organization's management assesses the security controls in their system and authorize (accredit) the system for operation.

Configuration Management (CM) ensures that operational personnel control changes to their system's configuration.

Contingency Planning (CP) ensures that operational personnel have a plan for continued operation to maintain availability of critical user and system-level information in emergency situations.

Identification and Authentication (IA) is the capability of the system to identify and verify (i.e., authenticate) system users, processes acting on behalf of users, or devices.

Incident Response (IR) ensures that operational personnel handle security incidents and promptly report incidents to appropriate authorities.

Maintenance (MA) ensures that operational personnel perform preventative and regular maintenance on their system.

Media Protection (MP) ensures that operational personnel restrict access to system media to authorized personnel and physically control system media in controlled areas.

Physical and Environmental Protection (PE) ensures that operational personnel limit physical access to systems and protect systems against environmental hazards.

Planning (PL) ensures that the organization's management develops and implements a security plan for the system.

Personnel Security (PS) ensures that operational personnel are trustworthy and meet security criteria for their positions.

Risk Assessment (RA) ensures that the organization's management assesses the risk and magnitude of harm that may result from security attacks on the system.

System and Services Acquisition (SA) ensures that the organization's management allocates the resources required to adequately protect their system.

System and Communications Protection (SC) is the capability of the system to monitor, control, and protect communications and includes architectural controls, confidentiality, data integrity and interoperability.

System and Information Integrity (SI) ensures that operational personnel remediate system flaws, provide protection from malicious code and other attacks on the system's integrity, and monitor alerts and advisories and take appropriate action in response.

2. 2 Realization of Security Services through Controls

Table 2-1 depicts a mapping from the CAR/SAM System Security Policy to the controls identified in section 2.1.

Table 2-1. Mapping of Controls onto Asia/Pac System Security Policy

Asia/Pac system Security Policy	Technical Controls	Operational Controls	Management Controls
Confidentiality			
(a) ATN data shall be protected from unauthorized disclosure during processing, transmission, and storage commensurate with the designated sensitivity of the data.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE)	System and Services Acquisition (SA)
Data Integrity			
(a) ATN data shall be protected from unauthorized or undetected modification during transmission, storage, and processing.	System and Communications Protection (SC)	System and Information Integrity (SI) Physical and Environmental Protection (PE)	
Authenticity			
(a) ATN users and processes shall be uniquely identified.	Identification and Authentication (IA)	Personnel Security (PS)	System and Services Acquisition (SA)
(b) ATN users and processes shall be authenticated before being granted access to ATN data, services, and resources.	Identification and Authentication (IA) Access Control (AC)	Personnel Security (PS)	
(c) ATN data, services, and resources shall be protected from unauthorized use or tampering.	Access Control (AC)		

Asia/Pac system Security Policy	Technical Controls	Operational Controls	Management Controls
(d) ATN users and processes shall have access only to those ATN data, services, and resources for which they have authorization.	Access Control (AC)		
Availability			
(a) ATN data, services, and resources shall be available for use by authorized users and processes.	System and Communications Protection (SC)	System and Information Integrity (SI) Contingency Planning (CP) Incident Response (IR) Physical and Environmental Protection (PE) Personnel Security (PS)	System and Services Acquisition (SA)
Accountability			
(a) An audit trail of use of ATN data, services, and resources by ATN users and processes shall be maintained.	Audit and Accountability (AU)	Personnel Security (PS)	
Verification			
a. ATN systems shall be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources.			Planning (PL) Risk Assessment (RA)
Authorization			
a. ATN systems shall be formally approved for operation by the cognizant Designated Approving Authority (DAA).			Certification, Accreditation, and Security Assessments (CA)
b. Significant changes to ATN systems shall require another formal approval (or re-authorization).			Certification, Accreditation, and Security Assessments (CA)

3. MANAGEMENT CONTROL GUIDANCE

As defined is section 1.1, Management Controls are safeguards or countermeasures that focus on the management of risk and the management of system security.

3.1 Certification, Accreditation, and Security Assessments (CA)

The CAR/SAM System Security Policy requires that ATN systems be verified to have system security commensurate with the risk and magnitude of harm resulting from unauthorized disclosure, modification, or deletion of ATN data, or unauthorized use and denial of service of ATN services and resources. This requirement essentially says that a system should have controls in place to meet the fundamental objectives for system security as noted in section 1.1. Verification of system security is more generally termed certification. This is where an organization conducts a risk assessment (see 3.3) and an assessment of the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome in terms of meeting the fundamental system security objectives. Management may use the CAR/SAM System Security Checklist [Asia/Pac SSC]as a general guide in assessing security controls.

The CAR/SAM System Security Policy also requires that ATN systems be formally approved (i.e., accredited) for operation by an individual responsible for security in the organization. This individual is called the Designated Approving Authority (DAA). The DAA is a senior organizational official that signs and approves the security accreditation thereby authorizing operation of the system.

3.2 Planning (PL)

A system may be authorized for operation by the organization's management even though there are controls not in place or controls which could be enhanced as determined by the security verification process. In this situation the organization would develop and implements a security plan for adding or enhancing controls in the system.

3.3 Risk Assessment (RA)

A formal risk assessment is the process by which an organization determines the risk and magnitude of harm resulting from unauthorized. The general process of risk assessment is depicted in Figure 3-1 from [NIST 800-100]. The process begins (1) with a characterization of the system. This involves identifying the data, resources, and services, that constitute the system and determining the importance of these items to the organization. The next steps are to identify threats to (2) and vulnerabilities of (3) the data, resources, and services. Identifiable threats (e.g., disclosure, modification, or loss of data) will have some probability of occurring

and causing loss or damage to a system. An analysis (4) of the threats and vulnerabilities should be conducted following a structured approach to analyze controls, estimate likelihood of threat occurrence, and assess the potential impact of the threats to arrive at a general risk determination. Risk analysis are generally and qualitative (e.g., high, medium, low). For each identifiable threat one or more controls should be recommended (5). The nominal controls in the CAR/SAM System Security Checklist [Asia/Pac SSC] may be used as a general guide; however, additional system specific controls may also be necessary. The overall results of the risk assessment should be formally documented (6).

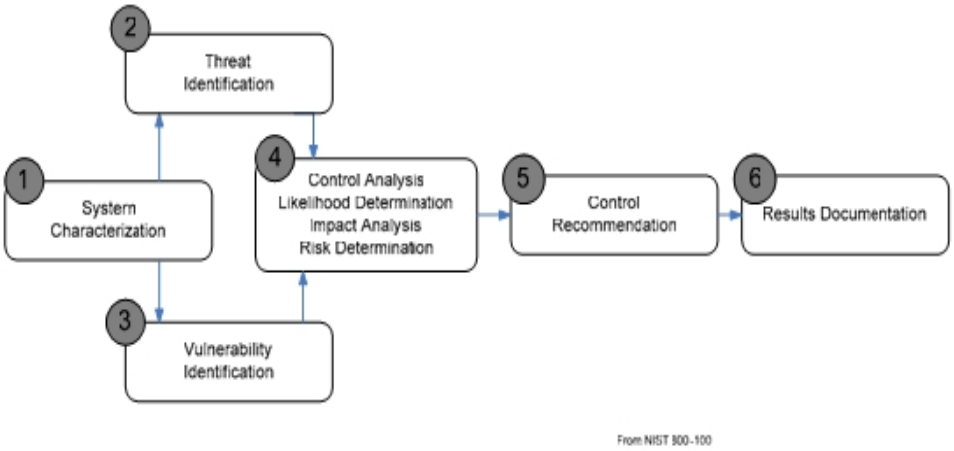


Figure 3-1. Risk Assessment Process

3.4 System and Services Acquisition (SA)

System and Services Acquisition (SA) is the control whereby an organization's management allocates the resources required to protect the system to level commensurate with the risks to the system. This activity should be applied as part of an on-going security policy for the organization. Specific resources should be allocated as a result of the CA and RA activities.

4. OPERATIONAL CONTROL GUIDANCE

As defined is section 1.1, Operational Controls are safeguards or countermeasures for a system that are primarily implemented and executed by people.

4.1 Awareness and Training (AT)

Awareness and Training (AT) is the control for disseminating security information that management and operational personnel need to do their jobs. Awareness and Traning ensures that management and operational personnel understand their security responsibilities and therefore are able to properly use and protect the system data, resources, and services.

4.2 Configuration Management (CM)

Configuration Management (CM) is the control that ensures that operational personnel control changes to their system's hardware components, software components and system adaptation parameters. Figure 4-1 depicts the Configuration Management process.

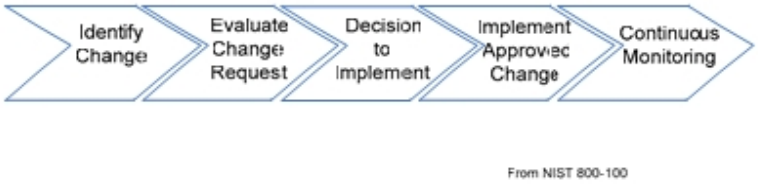


Figure 4-1. Configuration Management Process

The first step in the process is to identify the need for the change. There can be various reasons for change such as the need to support more bandwidth on a communication channel, the need to upgrade to a new Operating System if the current is no longer supported, and general functional enhancements or corrections to the system. The change should be submitted to a decision-making body in the organization, e.g., to a Configuration Control Board (CCB).

The next step is to evaluate the change request. An impact assessment should be conducted to determine the effect of the change to the system under change or to other interrelated systems. For example a change in the routing policy could effect all systems in the network. Thus a change needs to be evaluated to determine if it is technically correct and if the gains (performance, new functionality, etc) are cost effective.

Next the CCM must make a decision to implement. The CCB may approve, deny, or otherwise defer implementation of the change.

If a decision to implement the change is made, then it should first be tested in an off-line or test environment. Once tested the change may be placed into the operational system and the associated configuration control documentation is updated.

Configuration Management does not actually start and stop with incremental changes. Rather it is an on-going process that requires continuous monitoring. Configuration Management requires that operational personnel are always aware of their current baseline (for example a specific software release) and that the system is observed in operation to determine if there is any degradation in functional or performance capabilities as the system baseline is changed. In addition to managing software releases, application of fixes (i.e. "patches") to the system and changes in adaptation parameters must also be managed and continuously monitored.

4.3 Contingency Planning (CP)

Contingency Planning (CP) is the control that ensures that operational personnel have a plan for continued operation to maintain availability of critical user and system-level information in emergency situations. Figure 4-2 from [NIST 800-34] depicts the Contingency Planning Process.

Figure 4-2. Contingency Planning Process

The organization should firstly have a policy for contingency planning that establishes the overall contingency objectives. There should be an impact analysis that evaluates the potential loss of a system or service. This may be the same as the system characterization in the Risk Assessment. The Preventive Controls are a subset of the overall CA controls which address the specific loss of systems and services. A recovery strategy should exist for each potential system/service loss. All the previous steps go into developing a formal Contingency Plan. Attachment A contains an outline for a Contingency Plan. Operational personnel should plan to test the Contingency Plan. Training should be conducted as necessary and actual exercises such as operation of backup systems should be conducted. As the system changes the contingency plan must be updated as part of a Plan Maintenance program.

4.4 Incident Response (IR)

Incident Response (IR) is the control that ensures that operational personnel handle security incidents and promptly report incidents to appropriate authorities. Figure 4-3 from [NIST 800-61] depicts the Incident Response Life Cycle.

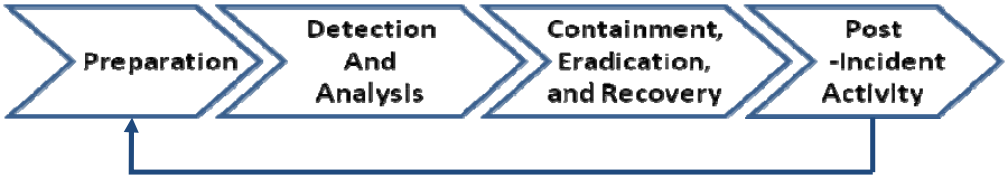


Figure 4-3. Incident Response Life Cycle

As depicted in Figure 4-3, Incident Response has several phases ranging from initial preparation through post-incident analysis which feeds back into the preparation phase. During preparation the organization selects and implements controls based on their risk assessment. The controls however cannot guarantee absolute protection and there will always be some residual risk. Therefore detection is required to alert the organization that an incident has occurred. Detection is primary through the technical controls described in section 5. When detected appropriate personnel within and external to the organization must be promptly notified. When an incident does occur, operational personnel can minimize the impact by firstly containing it before it spreads and does further damage. Measures should be taken to eradicate it as soon as possible so that recovery to normal services can be achieved. The post-incident analysis should attempt to identify the source of the incident as well as determine what additional controls can be implemented to prevent future occurrences, i.e., to apply "lessons learned" from the incident.

Attachment B contains an outline for an Incident Response Plan.

4.5 Maintenance (MA)

Maintenance (MA) is the control ensures that operational personnel perform preventitive and regular maintenance on their system.

4.6 Media Protection (MP)

Media Protection (MP) is the control ensures that operational personnel restrict access to system media to authorized personnel and physically control system media in controlled areas.

4.7 Physical and Environmental Protection (PE)

Physical and Environmental Protection (PE) is the control ensures that operational personnel limit physical access to systems and protect systems against environmental hazards.

4.8 Personnel Security (PS)

Personnel Security (PS) is the control that ensures that operational personnel are trustworthy and meet security criteria for their positions.

4.9 System and Information Integrity (SI)

System and Information Integrity (SI) is the control that ensures that operational personnel remediate system flaws, provide protection from malicious code and other attacks on the system's integrity, and monitor alerts and advisories and take appropriate action in response.

5. TECHNICAL CONTROL GUIDANCE

5.1 Technical Controls

As defined in section 1.1, Technical Controls are safeguards or countermeasures that a system executes through mechanisms in the hardware or software components of the system itself. The technical controls addressed in this section are:

- AC - Access Control
- AU - Audit and Accountability
- IA - Identification and Authentication
- SC - System and Communications Protection

For the Management and Operational controls, general guidance was provided for each control. In this section Technical Controls are described in terms of the hardware or softwre components of the system to which they apply.

5.2 Technical Controls Applied to Information System Components

Technical Controls are best applied following a *Defense-in-Depth* strategy whereby multiple overlapping protection approaches are implemented. For the Asia/Pac ATN, this section provides guidance on the application of controls to the network, equipment, operating system, applications, and data. Figure 5-1 depicts the concept of Defense-in-Depth.

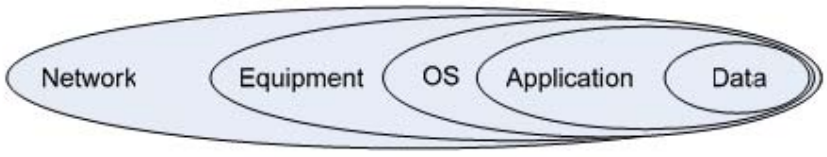


Figure 5-1: Defense-in-Depth

Figure 5-2 depicts the general technical contols applied to information system components.

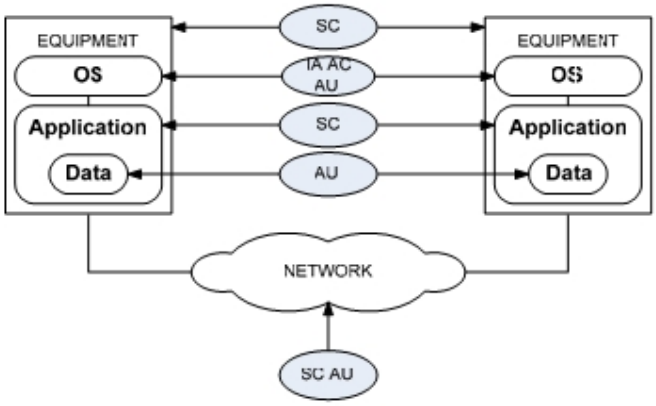


Figure 5-2: Technical Controls to ATN Component Mapping

As is depicted in Figure 5-2, the System and Communications Protection (SC) and Audit and Accountability (AU) control families apply to the Network. Note that network is used in a logical sense here so that protocol software in host systems is part of the network. The System and Communications Protection (SC) control family also applies to equipment. This generally refers to architectural controls. The Access Control (AC), Audit and Accountability (AU), and Identification and Authentication (IA) control families apply to the Operating System. The Systems and Communications Protection (SC) control family applies to Applications, and the Audit and Accountability (AU) applies to Application Data.

5.2.1 Controls Applied to the Network

This section identifies network controls which may be applied in the Asia/Pac ATN in support of AMHS. Figure 5-3 provides an overview of the controls.

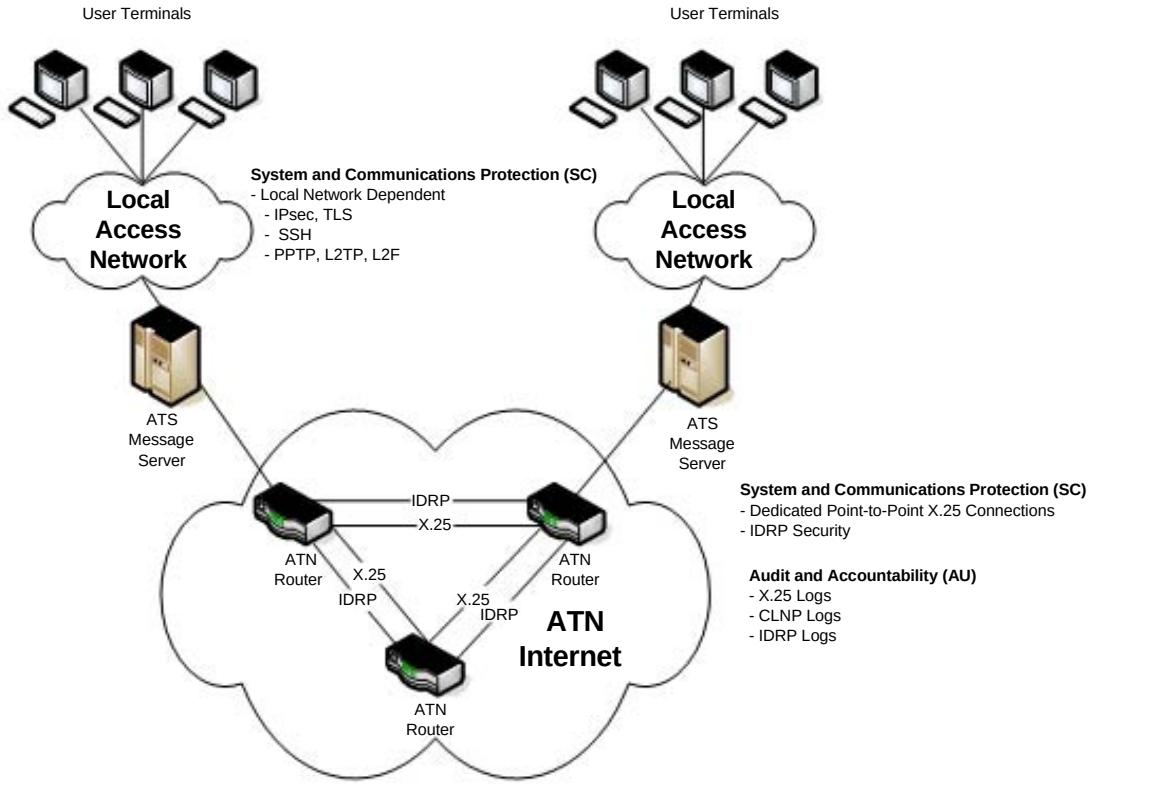


Figure 5-3: Network Controls

5.2.1.1 System and Communications Protection (SC)

5.2.1.1.1 Dedicated Point-to-Point X.25 Links

Currently interconnectivity in the Asia/Pac ATN Internet is through the use of dedicated pointto-point X.25 circuits. This limits access since X.25 circuits are associated with a specific physical port.

5.2.1.1.2 Inter-domain Routing Protocol Security

The Inter-domain Routing Protocol (IDRP) has defined options for authentication of routing data. Edition 3 of Doc 9705 defined a method of authentication using the HMAC keyed message authentication code. Edition 3 allows for two ATN routers to exchange public keys in public key certificates during the IDRP open

exchange.

Rather than exchange certificates and implement a supporting Public Key Infrastructure (PKI) it is recommended that the routers derive a shared session key from a pre-shared value.

5.2.1.1.3 Local Access Network Security

The connection of User Terminal to the AMHS switching systems is a local matter. These connections may be secured in a number of ways.

One common method is to use the Secure Shell (SSH) protocol. SSH contains secure replacements for several unencrypted application protocols such as telnet, rcp, and FTP.

An alternative to SSH for HTTP type applications is to use Transport Layer Security (TLS). All major web-browsers support TLS. TLS authentication is typically one way, authenticating the client to a server.

If the local access network is an IP network then an IPsec Virtual Private Network may be used to secure Terminal to AMHS communications.

If the local access method is not a layer 3 network, then various Level 2 protocols may be used. Options include the Point-to-Point Tunneling Protocol (PPTP), the Layer 2 Tunneling Protocol (L2TP), and Layer 2 Forwarding (L2F).

5.2.1.1.4 IPsec with the IP SNDCF

In the ATN Internet of the future the Internet Protocol Subnetwork Dependent Convergence Function (IP SNDCF) may be used to interconnect ATN routers in place of X.25 links. In this case, it is recommended that the IP Security (IPsec) protocols be used. This may be with manual key establishment or dynamically using the Internet Key Exchange (IKE) protocol. IKE may be used with pre-shared keys or using public key certificates.

5.2.1.2 Audit and Accountability (AU)

5.2.1.2.1 System Logs

It is recommended that the communication logs of Asia/Pac ATN Routers be reviewed for anomalous activity. Specifically the following logs should be reviewed:

- X.25 Logs
- IDRP Logs
- Connectionless Network Protocol (CLNP) Logs

5.2.2 Controls Applied to Equipment

5.2.2.1 System and Communications Protection (SC)

5.2.2.1.1 Redundancy

Equipment may be configured redundantly to limit the effects of many attacks on systems including Denial-of-Service attacks.

5.2.3 Controls Applied to the Operating System

5.2.3.1 Identification and Authentication (IA)

5.2.3.1.1 User IDs and Passwords

System Administrators may configure the allowed users of the system. There are at least two classes of accounts which may be configured: normal system users and superusers.

5.2.3.2 Access Control (AC)

5.2.3.2.1 User Access

Once users have been identified and authenticated using IA controls, the system administrator may limit their operating environment, that is, an administrator may limit the types of transactions and functions that authorized users are permitted to exercise.

5.2.3.2.2 OS Checklists

The National Institute of Standards and Technology (NIST) maintains a Security Configuration Checklist Repository for various products and systems including all major Operating Systems. (http://checklists.nist.gov/repository/category.html)

5.2.3.3 Audit and Accountability (AU)

5.2.3.3.1 OS System Logs

The operating system logs should be reviewed on a regular basis for abnormal activity. This may be done manually or using automated tools such as TRIPWIRE.

5.2.4 Controls Applied to Applications

5.2.4.1 System and Communications Protection (SC)

5.2.4.1.1 AMHS Security

Figure 5-4 depicts AMHS Security which is applied from an originating ATS Message User Agent to a destination ATS Message User Agent.

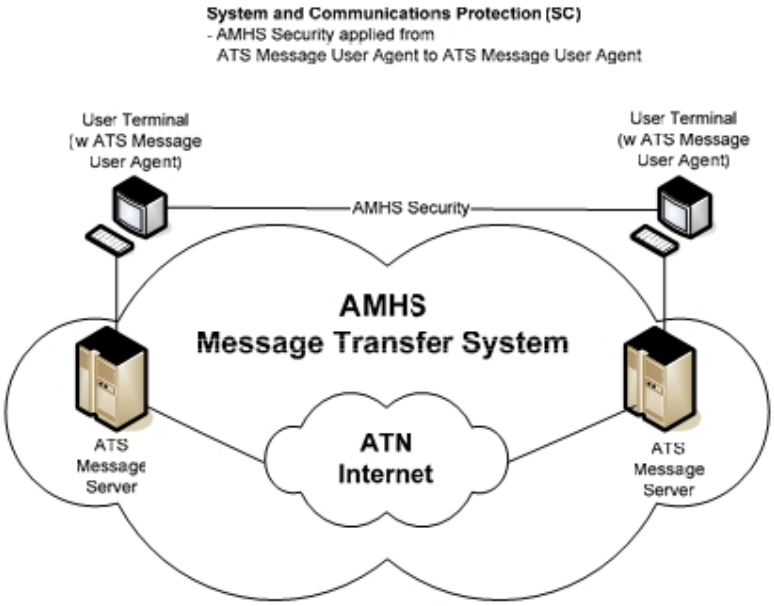


Figure 5-4: AMHS Security

AMHS security begins with the originating ATS Message User Agent digitally signing an Interpersonal Message using its Private Key. The message is sent throught the ATS Message Transfer System to the recipient ATS Message User Agent. The receipient UA retrieves the Public Key of the originating UA from a public key certificate using a supporting directory service. With the originators public key the recipient UA can verity the signed message.

5.2.5 Controls Applied to Data

5.2.5.1 Audit and Accountability (AU)

5.2.5.1.1 AMHS Traffic Logging

Traffic Logging is required as part of the basic AMHS service. Specifically, Doc 9705 requires that "an AMHS Management Domain shall be responsible for long-term logging of all messages in their entirety which are originated by its direct AMHS users, for a period of at least thirty days."

6. References

[Asia/Pac SSP] ASIA/PAC Aeronautical Telecommunication Network System Security Policy, Second Edition, September 2008

[Asia/Pac SSC] ASIA/PAC Aeronautical Telecommunication Network System Security Checklist, First Edition, May 2009

[NIST 800-34] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems"

[NIST 800-53] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems"

[NIST 800-61] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, "Computer Security Incident Handling Guide"

[NIST 800-100] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, "Information Security Handbook: A Guide for Managers"

ATTACHMENT A
CONTINGENCY PLAN OUTLINE

1. INTRODUCTION

1.1 Purpose

1.2 Applicability

1.3 Scope

1.4 References

[NIST 800-34] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, "Contingency Planning Guide for Information Technology Systems", June 2002

2. CONCEPT OF OPERATION

2.1 System Description

2.2 Line of Succession

2.3 Responsibilities

3. NOTIFICATION/ACTIVATION

3.1 Notification Procedures

3.2 Damage Assessment

3.3 Plan Activation

4. RECOVERY

4.1 Sequence of Recovery Activities

4.2 Recovery Procedures

5. RECONSTITUTION

ATTACHMENT B
INCIDENT RESPONSE PLAN OUTLINE

1. INTRODUCTION

1.1 Purpose

1.2 Applicability

1.3 Scope

1.4 References

[CSIRT] Carnegie Mellon Software Engineering Institute "Handbook for Computer Security Incident Response Teams (CSIRTs)", April 2003

[NIST 800-61] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, "Computer Security Incident Handling Guide", January 2004

[RFC 2196] Fraser, B. Ed., "Site Security Handbook", September 1997

[RFC 2350] Brownlee, N., and E. Guttman , "Expectations for Computer Security Incident Response", June 1998

2. Contact Information

2.1 Name of the Team 1

2.1.1 Team Member 1

Address

Time Zone

Telephone Number

Facsimile Number

Other Telecommunication

Electronic Mail Address

Public Keys and Encryption Information

Other Information

2.1.n Team Member n

2.x Name of the Team x

3. Charter

3.1 Mission Statement

3.2 Constituency

3.3 Sponsorship and/or Affiliation