A Common Mobility Solution for ATN OSI and Internet Protocol Stacks

Tom McParland, BCI: tmcparland@bcisse.com

Abstract: The ATN as a global aviation infrastructure provides communications service to different classes of safety and non-safety related users over different air-ground subnetworks. The ATN provides mobility and segregates traffic using the OSI IDRP routing protocol and CLNP packet forwarding protocol. Non-safety related services such as those envisioned for the "Airborne Internet" could be rapidly developed using the Internet "TCP/IP suite of protocols". To accommodate emerging IP traffic, this paper advocates using the ATN OSI IDRP routing protocol to advertise IP routes and thus provide a common mobility solution.

ATN Traffic

The Aeronautical Telecommunication Network (ATN) is intended to be a global infrastructure that will, "extend the information superhighway to the world of aviation". The ATN is primarily designed to carry operational traffic representing safety and regularity of flight. The ATN operational traffic type consists of two distinct the traffic categories: Air Traffic Services (ATS) communication and Airline Operational Control (AOC) communication. ATS communication is related to air traffic services including air traffic control, aeronautical and meteorological information, position reporting and other services related to safety and regularity of flight. ATS communication involves one or more air traffic service administrations. AOC communication occurs between the aircraft and an airline operations centre or airport and is required for the exercise of authority over the initiation, continuation, diversion or termination of flight for safety and regularity as well as for efficiency reasons. The ATN however is not limited to operational traffic. The ATN as a global infrastructure is also intended to carry aeronautical administrative communications (AAC) and provisions are made to carry General Communications. The General Communications type of traffic includes Airline Passenger Communications (APC), which is defined as communication relating to the non-safety voice and data services to passengers and crewmembers for personal communication. [1]

This notion of a common infrastructure is generally recognized and promoted by the aviation community. In particular, it is recognized that, "a communications infrastructure providing safety and non-safety services without degradation in QOS for safety communications could provide significant economic efficiencies". Therefore, "to the extent that it is technically and institutionally feasible the infrastructure supporting the ATS communications should also be capable of supporting the non-ATS communications". [2] Simply stated, it makes sense that the ATN should support non-ATS communications including services such as those envisioned under the Airborne Internet. [3]

ATN Protocol Stack

The ATN standards as specified by the International Civil Aviation Organization (ICAO) define a set of specific applications and a general purpose set of communication services, which allow ground, air-to-ground and avionics data sub-networks to interoperate by adopting common interface services and protocols. The ATN standards are based on the OSI protocol suite rather than the Internet Engineering Task Force (IETF) suite informally referred to as the "TCP/IP protocols". The reasoning at the time was that the OSI protocols were more formally specified and included such things as detailed protocol implementation conformance matrices and combinations of functions at each protocol level called profiles, and thus were more suitable for avionics certification. In addition, the primary contributing administrations to ICAO were still promoting the OSI stack. In the US, in particular, the National Institute of Standards and Technology had developed the Government Open Systems Interconnection Profile (GOSIP). However, as is common knowledge, the TCP/IP protocols have long since been proven in the World Wide Web and therefore are able to offer potential economic benefit and provide for the rapid introduction of new services in the global aviation environment.

ATN Applications and Upper Layer Service

The air-ground applications specified in the ATN standards are: Controller Pilot Data Link Communications (CPDLC), Automatic Dependent Surveillance (ADS), and Flight Information Service (FIS). The ATN standards specify Application Service Elements (ASEs) for each application. The ASEs are combined with other upper layer components to form a complete application entity (AE). An AE is the part of the overall application concerned with communications. In support of the ATS air-ground applications, the ATN has defined the Upper Layer Communication Service (ULCS). The ULCS provides a streamlined upper layer architecture using a "fast byte" approach. This approach essentially reduces the OSI session and presentation layer to the exchange of a single byte of information during session establishment. The ULCS has been enhanced in Edition 3 of the standard to provide end-to-end security. It is worth noting that the ULCS also provides a Generic ATN Communication Service (GACS). GACS provides a vehicle for migration of legacy applications; in particular, legacy AOC applications could use GACS and take advantage of the end-to-end security provisions.

The ATN standards specify two ground-ground applications: AMHS and AIDC. AMHS is the ATS Message Handling Service. AMHS is based on X.400 standards and is intended to replace the Aeronautical Fixed Telecommunication Network (AFTN). AMHS runs over the full OSI upper layer stack. AIDC is the ATS interfacility data communication service. AIDC is currently defined with its own upper layer communications service, which is functionally equivalent to the air-ground ULCS for those features required in the ground-ground environment. Ground-ground applications are not addressed in this paper; however, it is interesting to note that certain ICAO regions are considering running the AMHS X.400 upper layer stack directly over an IP Internet.

ATN Internet Communications Service

The other communications service and the subject area of this paper is the ATN Internet Communications Service. The ATN transport and network layer comprise the ATN ICS. The ATN specifies the OSI TP4 protocol to provide essentially the same end-to-end transport service as TCP. The OSI Connectionless Network Protocol (CLNP) is specified to provide the same network service as IP, namely a hop-by-hop packet forwarding capability.

A basic objective of the ATN is to provide mobility, that is, to maintain transparent connectivity among ground-based applications and airborne counterparts. This connectivity is to be accomplished over multiple subnetwork types. The ATN currently recognizes a limited set of subnetworks: SSR Mode Select (Mode S), Very High Frequency (VHF) Digital Link (VDL), Aeronautical Mobile Satellite Service (AMSS), Gatelink, and High Frequency (HF); however, the standard has a provision to add additional subnetwork types. There are a number of next generation aviation subnetworks, which are becoming or soon will become available. These subnetworks include enhanced SATCOM networks, commercial broadband aviation networks for air-ground communications, and wireless networks for airport area communications.

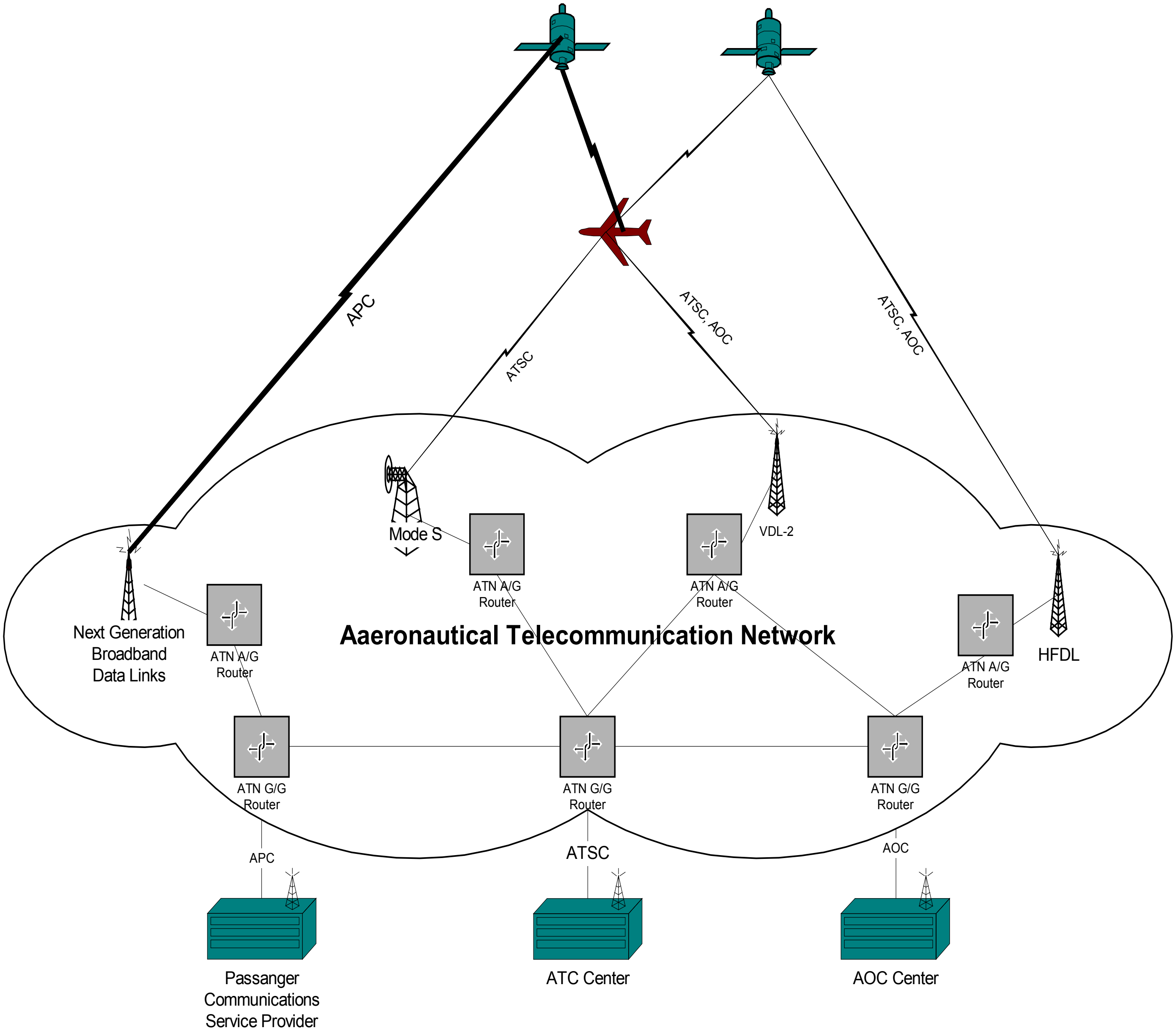
The ATN ICS is what permits the ATN to serve as a "network of subnetworks". A fundamental feature of the ATN is segregation of the various traffic types over different subnetworks. Segregation of traffic types ensures that application data passed over Air/Ground data links conforms to national and/or ITU restrictions applicable to that Air/Ground data link. The ATN standards distinguish the following traffic types: ATN Operational Communications - ATSC, ATN Operational Communications - AOC, ATN Administrative Communications, ATN Systems Management Communications, and General Communications, which as noted above includes APC. Figure 1 depicts the segregation of traffic types over various subnetworks.

How does the ATN support mobility?

Mobility in the ATN is essentially a problem maintaining one or more paths from ground automation systems to and from peer avionics systems, and exchanging data over these paths. Basically it is a routing problem and in particular it is a route maintenance problem. Route maintenance refers to the update of the routing database. The routing database is accessed by the forwarding protocol (i.e., CLNP or IP) to move data packets through the network on a hop-by-hop basis. If we consider the general approaches to route maintenance it is immediately obvious that static routing cannot support mobility. This is because routes to an aircraft are inherently dynamic in that an aircraft may traverse multiple subnetworks and within each subnetwork they traverse multiple ground stations. Thus we are left with some type of adaptive routing.

Figure 1

ATN TRAFFIC TYPE SEGREGATION



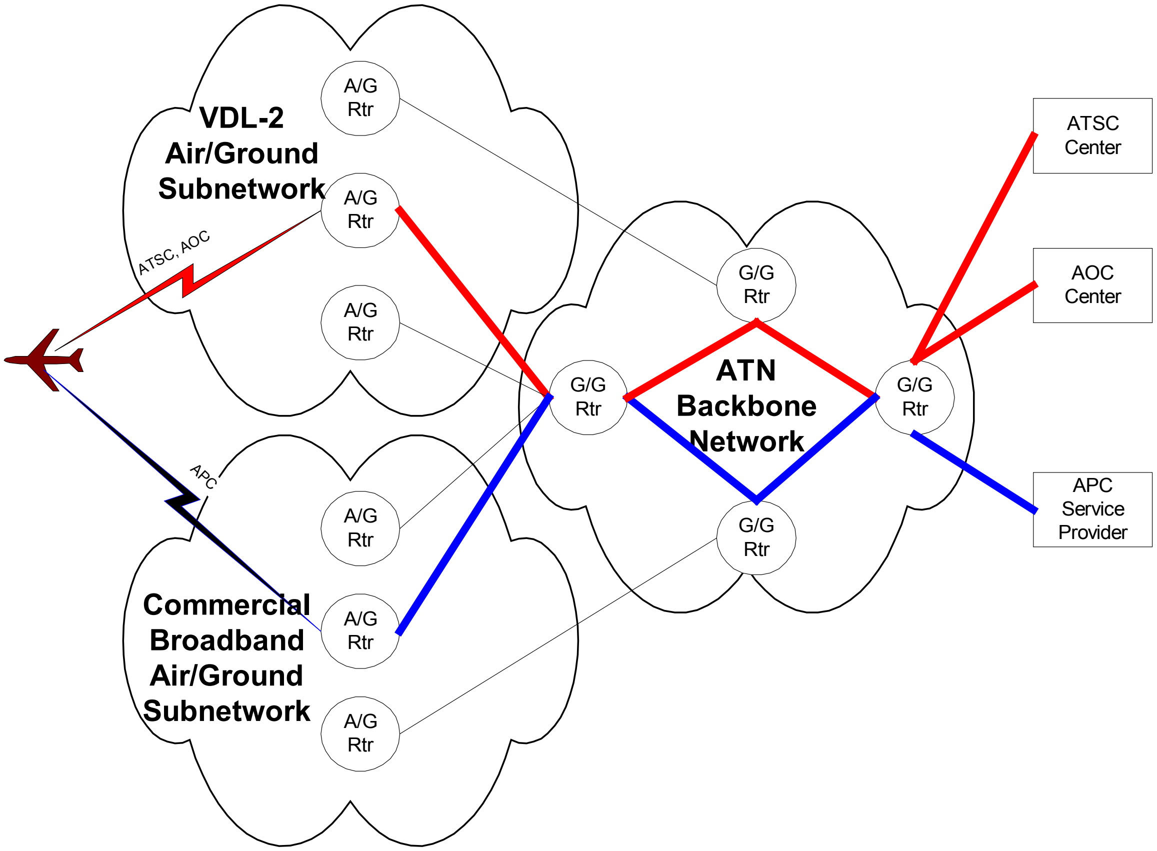
In general, adaptive routing may be centralized or distributed. A centralized approach to adaptive routing has the problem that the central control center where changes would be reported becomes a bottleneck, especially in a global environment. Even if enough capacity could be provided, there are associated timing considerations since a reported change in an aircraft's location must be available to communicating ground systems in real time. There are also administrative considerations with centralized adaptive routing. These considerations include determining which administration (a particular CAA, service provider, etc.) would operate the central control center and what are the liabilities associated with such an operation. Accordingly, since neither static routing nor centralized adaptive routing would be appropriate, we are led to some type of distributed adaptive routing approach as the solution to mobility.

There are two general approaches to distributed adaptive routing [4]. The approaches are based on the type of algorithm employed by the routing protocol. The first is called *link state* routing and it is based on some variation of Dijkstra's shortest path first algorithm [5]. The second is called *distance vector* routing and it is based on some form of the Bellman-Ford algorithm. This algorithm, originally developed by R.E. Bellman [6], is known though its description by L.R. Ford and D.R. Fulkerson [7] as applied to the problem of flows in networks. Under link state routing, each change in the network topology (in connectivity to an aircraft in the context of support for mobility) is broadcast to every other node in the network. Upon receipt of each change message, each node updates its image of the network topology and calculates the complete (shortest) path to the destination in the change message. The main problem with this approach is that the number of messages required to report changes in network topology becomes inordinately large. Thus we are left with at a distance vector approach to distributed adaptive routing in the ATN.

The principle of distance vector routing is that specific changes in connectivity are propagated (i.e., advertised) to affected routers throughout the network. In its simplest form an advertised route is a vector containing a destination address and a distance metric, which is generically a measure of the cost associated with the path being advertised to a particular destination. The ATN routing protocol is the OSI Inter-Domain Routing Protocol. [8] It is essentially an enhanced distance vector protocol sometimes referred to as a "path vector" routing protocol. An IDRP router advertises routes with two components: network layer reachability information (NLRI) and path information. NLRI may be individual network addresses or aggregated addresses. Path information consists of a list of routing domains along the path to a destination identified by the NLRI and other path attributes, which are the unique characteristics of the path. For aircraft the NLRI is the unique address of the aircraft, called its NSAP address, and a particular path attribute (the security attribute) is used to signal the traffic type and subnetwork type of the route being advertised. For example, an aircraft with ATSC, AOC, and APC applications that has connectivity over both a VDL-2 and a commercial broadband subnetwork might advertise a route to the ATSC and AOC applications over VDL-2 and a route to APC applications over the commercial broadband subnetwork. These routes are propagated through the network to the routing domains of the ground applications.

With this general conceptual view of the process we can now see how mobility in the ATN is accomplished. As the aircraft moves into the coverage of a new Air/Ground router and out of the coverage of its current Air/Ground router, a new route with the appropriate security attribute (signaling traffic type and subnetwork type) is propagated through the network and the old route is withdrawn. One can visualize the process as there being different colored routes to the aircraft in each of the routing databases. Routes of one color may be used for one traffic type while routes of a different color route are used for a second traffic type. See Figure 2. When it comes time to forward packets of information over these routes the following occurs. The forwarding protocol in a router indexes the routing database using the destination address and the traffic type that is signaled in the security tag of the packet header. Once it finds a route matching the address and traffic type, i.e., the same color route, it sends the packet to the next router, i.e., the one from which it received the route. This process continues until the packet reaches the destination.

Figure 2 – Different Paths for Distinct Traffic Types



How does IDRP differ from the Internet's Border Gateway Protocol?

The inter-domain routing protocol for the Internet is the Border Gateway Protocol 4 (BGP-4). [9] And so the question naturally arises, "Why not use the Internet inter-domain routing protocol?" The answer is that BGP-4 does not have the required functionality.

A key functional difference between IDRP and BGP-4 is that IDRP has a built-in transport protocol. The IDRP transport provides for acknowledgement, retransmission, and sequencing. BGP-4 however, even though it does have a finite state machine to track the state of BGP connections, does not have a full-fledged transport but rather relies on the Internet transport protocol TCP. A direct consequence of this is that in its current form BGP-4 is not suitable for operation over Air-Ground Links since a transport connection cannot be pre-configured over which BGP can run.

The ATN IDRP protocol includes provision for authentication. The basic process is that Public Key certificates are exchanged when the connection is established via the OPEN exchange, a key agreement procedure is performed and subsequent UPDATE exchanges are protected with a Message Authentication Code (MAC). The MAC is performed over the IDRP message including the message sequence numbers, which are part of the IDRP transport. This provides protection from replay attacks. An equivalent function would need to be added to BGP-4 to make it suitable for operation over an Air/Ground link.

BGP-4 only defines a subset of the IDRP path attributes and does not support path attributes that have been adapted by the ATN to support mobile policies. In particular, BGP-4 does not have the security path attribute.

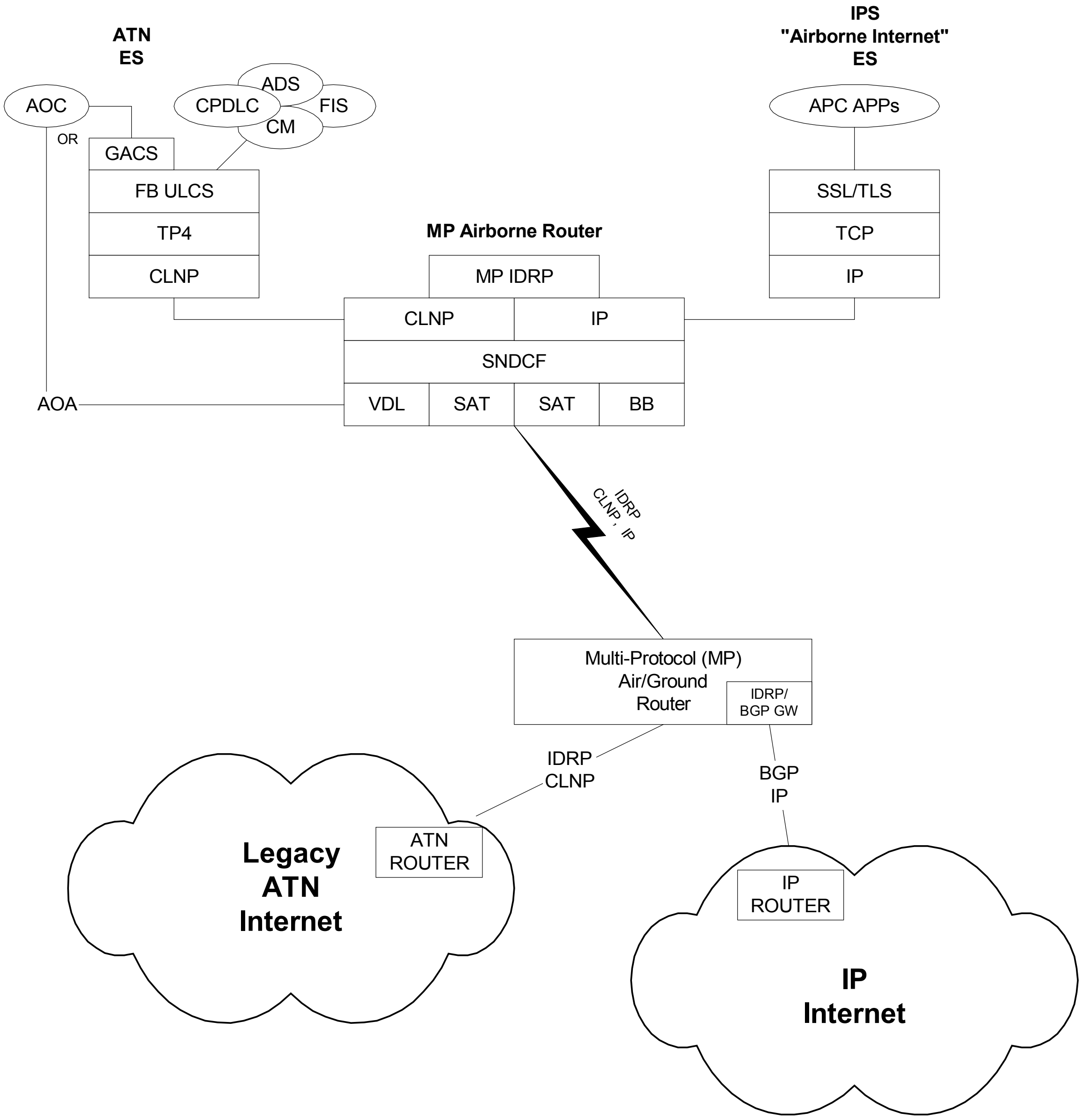
What is being proposed?

It is proposed that IDRP be used to advertise IP routes. The good news is that IDRP already provides for this. Specifically, the NLRI field in IDRP already allows non-CLNP routes to be advertised. It does not need an extension to do so as was the case for BGP-4. [10] Specifically the IDRP NLRI format is such that the identity of the protocol associated with the address information is contained in the NLRI thus permitting routes for protocols other than CLNP (ISO 8473) to be advertised. The IDRP standard considers the decision and forwarding process for use with protocols other than ISO 8473 outside of its scope. These items would need to be specified in the ATN standards.

What is the proposed environment?

In general what is advocated is the ATN Airborne and ATN Air/Ground routers optionally become multi-protocol routers. ATN Ground/Ground routers would not necessarily require modification as conforming IDRP implementations they may simply ignore NLRI for all protocols other than ISO 8473. (Re: 6.3.2 of [8]) However, it may be desirable in certain configurations to have this support. Figure 3 depicts a possible multi-protocol environment.

Figure 3 – Possible Multi-protocol Environment



There are two avionics end systems depicted. One is the ATN end system stack. The typical configuration for ATN applications (CPDLS, ADS, CM, and FIS) is to use the OSI Class 4 Transport (TP4) with the Fast Byte Upper Layer Communications Service (FB ULCS). Also depicted is the Generic ATN Communications Service (GACS) extension to the ULCS. As mentioned above, this permits legacy applications to use the ATN communication services including the upper layer security service; however, the common practice is that AOC applications are migrating to the AOC over AVLC (AOA) service.

The second avionics end system is an Internet Protocol Stack (IPS) end system. This stack is suitable for emerging applications generally associated with the "Airborne Internet" and similar initiatives and may be used for APC. This stack uses the Internet Transport Control Protocol (TCP). As depicted, Internet security services such as Secure Sockets Layer (SSL) and its successor Transaction Layer Security (TLS) may be applied. In fact, it may be possible to exploit the ATN security provisions. In particular, it would be possible to extend the ATN Key Agreement Scheme to establish keys for IDRP, the ATN ULCS and the Internet ES stack, for example, using the ATN cipher suites with TLS. [11] In other words, it may also be possible to have a "common security solution for ATN OSI and Internet Protocol Stacks".

The Multi-Protocol Airborne Router depicted in Figure 3 is a possible implementation of the proposed solution. Operation in this configuration is as follows. A join event is received from one of the air/ground subnetworks. An exchange of Intermediate System Hello (ISH) messages occurs to discover subnetwork addresses and associate them with corresponding CLNP NSAP addresses. If the subnetwork were configured to support IP traffic, then an association would also be made between a subnetwork address and the IP address. At this point IDRP is invoked to advertise routes for all traffic types on board the aircraft. In the example environment, this would include a route to APC applications. Upon receiving these routes, the Multi-Protocol Air/Ground router would advertise the CLNP routes to the rest of the "legacy ATN Internet" (which operates with IDRP and CLNP only). The Multi-Protocol Air/Ground router would advertise the IP routes using BGP. That is, a simple IDRP to BGP gateway would be implemented in the Multi-Protocol Air/Ground router. In this way standard off-the-shelf IP routers could be used for the IP Internet. In this example environment different traffic types are not segregated within the IP Internet. They would however continue to be segregated in the legacy ATN Internet.

What about using commercial broadband subnetworks for safety applications?

If the approach advocated in this paper were adopted, then commercial wide-band air/ground subnetworks could be used at least as a backup to the subnetworks reserved for use by aeronautical safety applications. In fact, the Air/Ground router could enforce the priority requirements (in Sub-Volume 1 of [1]) by giving priority to ATSC traffic over AAC and APC traffic. This would be consistent with the overarching objective of ensuring the availability of safety applications since having multiple alternative paths would increase availability. In this context it should also be kept in mind that the end-to-end integrity requirements of the ATN are above the network layer. Accordingly we can re-phrase the quote cited in the beginning of this paper by switching the "ATS" and "non-ATS" adjectives and maintain that, "to the extent that it is technically and institutionally feasible the infrastructure supporting the non-ATS communications should also be capable of supporting the ATS communications."

References:

[1] – International Civil Aviation Organization (ICAO) Document 9705, "Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN)", Ed. 3

[2] – Kors van den Boogaard, "AMCP 8 Report, non-ATS Communication", Aeronautical Mobile Communications Panel, Working Group C, 5th Meeting, Working Paper 16

[3] – A description of the "Airborne Internet" may be found at www.airborneinternet.com.

[4] – Information technology – Telecommunications and information exchange between systems – OSI Routeing Framework, ISO/IEC TR 9575, 1995

[5] – Dijkstra, E.W., "A note on two problems in connection with graphs", Numerical Mathematics, Vol. 1, 1959: 269-71

[6] – Bellman, R.E., *Dynamic Programming*, Princeton University Press, Princeton, NJ, 1957

[7] – Ford, L.R. and Fulkerson, D. R., *Flows in Networks*, Princeton University Press, Princeton, NJ, 1962

[8] - Information Processing systems – Telecommunications and Information Exchange between Systems – Protocol for Exchange of Inter-domain Routeing Information among Intermediate Systems to Support Forwarding of ISO 8473 PDUs, ISO/IEC 10747, 1993

[9] – Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995

[10] – Bates, T., Rekhter, Y., Chandra, R., and D. Katz, "Multiprotocol Extensions for BGP-4", RFC 2858, June 2000

[11] – Gupta, V., Blake-Wilson, S., Moeller, B., Hawk, C., and N. Bolyard, "ECC Cipher Suites for TLS", January 2004