EUROCONTROL

ATNP/WG2/
WP159/
15 August 1995

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Banff 9.10.95-13.10.95

Analysis of the Mobile IP Proposal and Comparison with ATN Mobile Routing

Presented By Henk Hof

Prepared by Tony Whyman

SUMMARY

This document analyses the Mobile IP specification currently under development by the Internet Engineering Task Force (IETF). The specification is compared with the ATN Routing Concept and conclusions drawn as to any ideas that may be usefully taken into the ATN Specification from the work on Mobile IP. Tutorial background information is provided on both Mobile IP and ATN Mobile Routing. The result of this analysis is the conclusion that while Mobile IP meets the requirements drawn up by the IETF for adding support for mobility to the Internet, it does not meet the ATN requirements for high availability and strong routing policies. There is therefore only limited possibility for learning from Mobile IP experience in the validation and operation of the ATN.

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	15-Aug-95	Issue 1.0	

TABLE OF CONTENTS

1. Introduction

1.1 Scope

This document analyses the Mobile IP specification currently under development by the Internet Engineering Task Force (IETF). The specification is compared with the ATN Routing Concept and conclusions drawn as to any ideas that may be usefully taken into the ATN Specification from the work on Mobile IP. Tutorial background information is provided on both Mobile IP and ATN Mobile Routing.

1.2 Purpose of Document

This analysis was prompted by a discussion on Congestion Management at the recent Rome ATNP/WG2 meeting. Copies of the Mobile IP working draft had been tabled and it was suggested that work being done on Mobile IP in respect of Congestion Management was relevant to the ATN Internet. Eurocontrol has taken on an action to investigate Congestion Management strategies by way of simulation. In preparing the specification this analysis has been performed in order to identify what, if anything, may be relevant to the ATN Congestion Management simulation. This analysis is. however, necessarily more general than just Congestion Management and also provides a comparison of the two approaches for supporting mobile systems

1.3 References

1.	draft-ietf-mobileip-protocol-11	IP Mobility Support
2.	draft-ietf-mobileip-optim-02	Route Optimisation in Mobile IP
3.	RFC 1256	ICMP Router Discovery Messages
4.	RFC 1520	Classless Internet Domain Routing (CIDR)
5.	RFC 1541	Dynamic Host Configuration Protocol
6.		ATN Draft SARPs - Part V - Internet Communications Service

2. Summary

Mobile IP has been developed to provide support for mobile users on the existing Internet with the goal of no change to the current infra-structure. In this, it appears to succeed and appears to be a good solution for (e.g) the laptop computer connected to a GSM network. However, there are many compromises in Mobile IP necessary to avoid changes to the existing Internet (no change to current Internet systems was a major design goal), and it does not appear to be comparable with the ATN, or indeed suitable for an operational network. Even in congestion management, where it has been suggested that there may be lessons in Mobile IP that can be adopted for the ATN, there is not really much in common. Indeed, congestion management solutions adopted for Mobile IP will only ever be in part applicable to the ATN, and may not even then be appropriate.

ATN Mobile Routing and Mobile IP are really two different specifications tackling different problems. The ATN is an operational network carrying safety related data, and with operators keen to minimise costs and control the use of mobile subnetworks. The ATN also has the advantage that there is no existing population of users to complicate the ATN specification.

On the other hand, Mobile IP is trying to add mobility on to a network infra-structure that offers no support for mobile systems and without changing that infra-structure. It is inevitably a compromise, with sub-optimal performance as a result. Robustness is not an overriding concern and neither is controlling cost or mobile subnetwork usage. The Internet is an environment where costs are shared and few users pay a direct cost for their use of network resources.

Superficially, Mobile IP and the ATN seem to be tackling the same problem and the question as to why they are different is a valid question for those who are not involved in the detail of the work. The answer is that they are not tackling the same problem and the resemblance is only superficial. They are different solutions for different problems and each is correct in its own environment.

Even on the subject of Congestion Management, where it has been suggested that there may be common cause, analysis has shown that there are different issues involved for Mobile IP. It is in fact very probable that the ATN can use the “standard” back-off procedures and that these will be fully acceptable. Even if there is value in responding to an indication that a mobile has changed its point of attachment, which appears to be the main issue affecting the ATN, in the ATN, this can realised in a straightforward manner, while, for Mobile IP, this is a major development task. This difference is simply due to Mobile IP’s use of the encapsulation mechanism, which is not a feature of the ATN

This is really a subject for validation activities which should:

i) Investigate whether, in a typical operational scenario, ATN performance is significantly affected by changes to a mobile’s point of attachment, and at what rate of change performance is affected.

ii) Investigate the impact of providing an indication to a sending End System (by way of a CLNP Error PDU) that a packet has been discarded due to a change in the point of attachment (indicated by error reason destination unreachable), and acting upon this indication to (a) forcing rapid recalculation of the round trip delay, and (b) overriding the back-off procedure.

There also appears to be a need to investigate the possibility of requiring cryptographic mechanisms for IDRP authentication procedures on air-ground data links.

When comparing Mobile IP to ATN Mobility, the following observations have been made during the analysis reported in the remainder of this paper:

1. Mobile IP is a very recently developed specification and has gone through a number of successive drafts over the last few months. It is based on preceding experimental mobile IP solutions, all of which were based on the notion of forwarding packets from a fixed reference point (the "Home Agent") to where the mobile is currently attached to the Internet. The forwarding mechanism depends on encapsulation of one IP packet within another, in order to work. The use of encapsulation is a necessary compromise, but one which introduces many weaknesses into Mobile IP, as discussed below.

   The ATN Mobile Routing Concept has been developed over a number of years and is now in trial systems. It is based upon the ISO standard for Inter-Domain Routing (IDRP), and uses the routing policy mechanisms built into IDRP in order to minimise the routing overhead in support of mobile routing. A two level structure of reference points (the Home and the ATN Island Backbone) is used for this optimisation. However, there is no requirement in the ATN Routing Concept to encapsulate packets between these reference points and the mobile, and hence is not affected by the encapsulation related problems that apply to Mobile IP.

2 T There is no support for routing policy in Mobile IP. The ATN employs extensive support for policy based routing in order to meet local and application requirements for the use of different network technologies.

3. Mobile IP is really about supporting Mobile End Systems. Although it can be extended to cover Mobile Routers, Mobile IP does not replace the need to additionally convey a routing protocol (e.g IDRP) between the mobile router and a ground based router, over the communications path established by Mobile IP.

   The ATN mobile routing concept has been specifically developed to support airborne routers, which can then support multiple avionics systems. There is no need for additional routing information exchange.

4. Mobile IP can make concurrent use of multiple data links to a mobile system. However, if it does so then every packet sent from a Home Agent to a mobile is duplicated and sent over all concurrent data links. This procedure has been specified in order to provide for a degree of robustness, but is consequential on there being no explicit mechanism to report that a mobile has left a given point of attachment when multiple concurrent data links are employed.

   The ATN is also specified to use multiple concurrent data links, but data is not duplicated and is sent over only one of the available data links. This data link is chosen according to local and application requirements and such concurrently available data links may simultaneous carry data belonging to different applications.

5. Congestion Management in Mobile IP is complicated by four factors:

   a) The possibility that mobile networks may lose packets more readily than equivalent ground based networks (on the assumption that a connectionless protocol such as PPP is used on the data link);

   b) Packet loss when a mobile changes its point of attachment to the Internet;

   c) Significant changes in the computed round-trip delay when a mobile changes its point of attachment.

   d) Encapsulation of IP packets between the Home Agent and a Mobile System;

   e) The goal of avoiding change to the existing Internet.

   Congestion Management on the Internet currently requires a sending Host Computer to "back-off" when it detects congestion, and the need to retransmit after packet loss is typically assumed to indicate that a network has become congested. The first two

factors above may thus cause false indications of congestion, hence incorrectly invoking the back-off procedure, and with the consequence that throughput is degraded. Sudden changes in the measured round-trip delay (item (c) above) may also affect the back-off algorithm resulting either in unnecessary invocation of back-off - if the timer is now much shorter than it should be - or a delay in re-transmitting a packet. Either effect will degrade throughput.

The last two factors then introduce problems in dealing with these problems. In particular, encapsulation of IP packets makes it very difficult (without predictive logic in the Home Agent) to pass any indication to the sender that a packet discard has happened for either of the first two reasons, and hence the back-off procedure should not be employed. To process such an indication would anyway require changes to the way existing Host Computers work and is in conflict with the goal of no change to the existing Internet.

It is thus probable that even if solutions are developed to overcome (d), this will be an optimisation rather than an integral feature and that sub-optimal throughput will be accepted for most Hosts, along with sub-optimal routing.

ATN End Systems are also expected to employ the same back-off algorithm as do Internet Hosts. However, only items (b) and (c) in the above list applies to the ATN. Encapsulation is not used on the ATN, and all ATN air-ground subnetworks are required to use reliable communications protocols. It is also arguable as to whether these items are an issue as, in the ATN, an individual mobile will only change their point of attachment at a relatively slow rate. For example, a single AMSS link will probably be used for an entire flight, and a Mode S subnetwork will typically be used for at least 30 minutes. Therefore, any degradation in throughput due to this factor is unlikely to be significant.

6. Mobile IP provides no support for the use of priority and the mapping of priority onto different subnetwork connections to the same mobile system. The ATN does provide support for priority and priority mapping on to subnetwork connections, in order to ensure that safety related applications are guaranteed a high availability even when the network is congested by data from non-safety related applications, or for other reasons.

7. Mobile IP offers a deliberately sub-optimal routing strategy in order to avoid changes to the existing Internet addressing plan and routing paradigm. All packets to a given mobile must be sent via its “Home Agent”, where they are encapsulated in another IP packet and then sent to where the mobile is currently located. While this can be compared to the ATN’s “Home” and “ATN Island Backbone Router” concepts, Mobile IP essentially requires a single “Home” worldwide. While a mobile can have multiple Homes in order to try and avoid the consequences of this, each of a mobile’s Home Agents must necessarily have a distinct IP Address, and the appropriate Home Agent (i.e. the one nearest the mobile) must be known in advance by the sender. This tends to negate the advantage of a Home Agent and requires a second (undefined) level of management for mobile systems.

   In contrast the ATN mobile routing concept ensures that packets are always sent via the best route available to a mobile, without the sender having to have any knowledge as to what this route is. The best route may be a direct route (e.g. if an aircraft is reachable via a mobile subnetwork attached to the same Routing Domain), via the nearest ATN Island Backbone (i.e. when the aircraft is attached to a mobile subnetwork on the same ATN Island), or via the “Home” (i.e. when the aircraft is flying in another part of the world). There are times when the best route may not be the most optimal, as a more direct route may exist than those described above. However, this was a trade-off necessary to avoid overloading the ATN with routing updates.

   The ATN Mobile Routing Concept also ensures that routers in an ATN Island’s Backbone or Home can be readily duplicated at different sites, and concurrently

interconnected by multiple alternate data links, in order to provide back-up and high availability.

8. While an optimisation to Mobile IP has been proposed, which permits a Home Agent to redirect a sender to where a mobile is currently attached to the Internet, this optimisation requires special procedures in the sender to implement it (i.e. is not compatible with the goal of no change to Internet infra-structure) and requires cryptographic security mechanisms, as the procedure of redirection is especially vulnerable to masquerade and replay attacks. The optimisation does not avoid the need for encapsulation.

9. Mobile IP also requires cryptographic security measures between a Mobile and its Home Agent in order to counter vulnerabilities to masquerade and replay attacks. This is consequential on a wide separation between mobile and Home across potentially hostile intermediate subnetworks.

   The ATN relays routing information to mobile systems on a hop--by-hop basis with each Routing Domain being responsible for ensuring its neighbour's credentials. Cryptographic procedures are available, if required, but in most cases are not expected to be necessary, as points of entry for an attacker are not usually present. However, when comparing Mobile IP to the ATN, a vulnerability on the air-ground network does appear to exist in the ATN, which may need to be countered by invoking IDRP authentication mechanisms on air-ground data links.

The remainder of this paper presents and discusses first Mobile IP and then the ATN Routng Concept

3. The Mobile IP Development

The Internet Protocol (IP) provides the common datagram format for the exchange of packets through the Internet. The Internet was originally developed around the ARPANET Wide Area Network, and the ARPANET was the Internet's core network with subsidiary local networks, "hanging off" this core network. The IP paradigm, Addressing Plan and Routing Strategy was originally developed for this operational model. Although the Internet has now moved away from the concept of a single core network, to an environment where multiple service providers may each provide core networking services, the original operational model is still a strong influence on the way addressing and routing is carried out in the Internet. There was no support for mobility in this operational model and the Mobile IP Specification has had to extend this model to provide for mobility without affecting existing users.

In order to understand how Mobile IP works and why it has been developed in the manner that it has requires some knowledge of how the current addressing and routing strategy in the Internet today. This is discussed below.

3.1 Internet Addressing

IP has a simple datagram format comprising an IP Header and user data, and the IP header contains the source and destination address and other control information used by Routers, when routing the packet through the Internet. The Destination Address is not only a name that uniquely identifies the destination, but addresses are also allocated in such a way as to enable routers to find the destination host without having to know where every Host is located on the Internet. The address syntax and allocation rules are crucial for ensuring that this can work.

The Internet uses a network oriented addressing plan. Each network is assigned a unique "network number" and Host Computers (i.e. End Systems) are allocated a unique Host Id relative to the network number of the network to which they are attached. Each Host's unique internet address is then simply formed by concatenating this network number and the assigned host id. In consequence, as internet addresses are thus network relative, if a Host Computer is attached simultaneously to more than one network, it has a separate, and possibly totally unrelated, internet address for each network to which it is attached. Similarly, if a Host Computer moves from one network to another, its internet address must change to one relative to the network to which it is newly attached.

Internet addresses are really port addresses rather than system addresses, identifying a point of network attachment rather than the Host Computer itself.

An Internet Address is specified to be a fixed 32-bit number. Within what is a relatively small addressing space, it is not possible to define an address syntax that reserves a big enough field for an appropriate Host Id field for large networks, that then leaves over enough "bits" to give a unique number to all networks that might be deployed. The Internet Addressing Plan therefore defines three address formats (classes), each with a different split between the size of the Host Id and the Network Number. Class A Internet Addresses allow for a 24-bit Host Id and a 7-bit network number; Class B allow for a 16-bit Host Id and a 14-bit network number; and Class C Internet Addresses allow for an 8-bit Host Id and a 22-bit network number. The syntax of each address class is illustrated in Figure 1.

The original idea was that big networks, (e.g. the ARPANET) use class A addresses, medium sized networks use Class B, and small networks use class C. In practice, Class C has often turned out too small, while class B is unnecessarily big for most organisations, and, as there are not many Class A network numbers, these have proved very difficult to obtain. In order to make better use of Class B Addresses, a procedure known as "subnetting" has been applied. This procedure tends to view the Class B Network Number as an organisation identifier rather than a network identifier, and subdivides the Class B

Host Id field into a subnetwork identifier and Host Id, with the actual division defined by a bitmap known as a subnet mask. Each such subnetwork is then identified by the organisation's Class B network number, and the locally assigned subnetwork id. The remaining bits are then used to identify each host relative to each subnetwork.

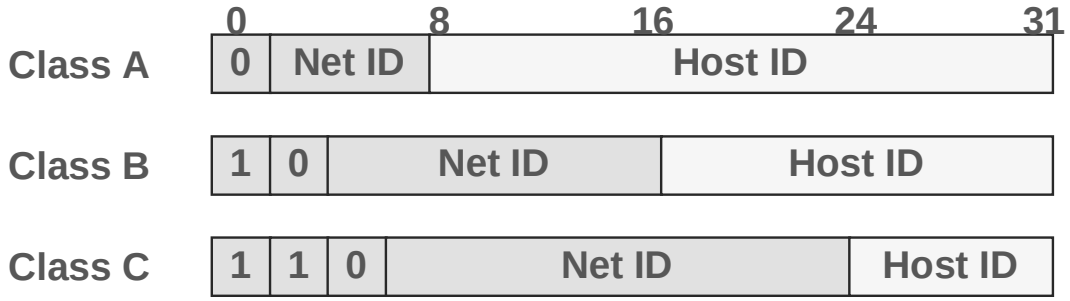

Figure 1 Internet Address Syntax

3.2 Internet Routing

Internet routing originally developed around class based addresses and network numbers. At the level of the ARPANET core, Core Gateways joined the ARPANET itself to the subsidiary non-core networks and the Core Gateways maintained routing tables that contained all assigned network numbers, which ones related to locally attached networks, which ones were reachable through other Core Gateways, and which ones were reachable through "non-Core Gateways" (i.e. local routers) on locally attached networks. This architecture is illustrated in Figure 2, where G1, G2 and G3 are examples of Core Gateways, and G4 and G5 are examples of non-Core Gateways.

Using their routing tables, the Core Gateways were able to route IP packets by extracting the destination network number from the destination address contained in each IP header and relating this either to another Core Gateway or a non-Core Gateway, on a locally attached network. The IP packet would then either be dispatched to the other Core Gateway, the destination Host on the locally attached network (identified by its Host id), or the identified non-Core Gateway. Non-Core Gateways would then similarly route IP packets, probably using the subnetwork identifier and the subnetting procedure.

While the Internet has moved away from the single Core Network and more sophisticated routing protocols have been developed to support this, the basic principle remains unchanged. Hence, Routers at the Core Gateway level in each Internet Service Provider must maintain a list of all assigned network numbers, which are assigned to locally attached networks and which are reachable through Routers in the same or another Service Provider. Network numbers have not been assigned with reference to Internet Service Providers or the topology of the Internet, and are essentially randomly distributed. There is thus no real scope for optimisation of router tables based on a presumption that whole blocks of network numbers are reachable through a given Service Provider or Router. Hence, routers at this level of the Internet have normally to keep routing information for each assigned network number,

This is not a scaleable routing architecture and is a recognised problem of the Internet today. While the Internet is generally running out of addresses, it is even more quickly exceeding the capacity of routers to handle all assigned network numbers.

To cope with this problem in the near term, a strategy known as Classless Inter-Domain Routing (CIDR) is being introduced. This strategy makes use of some unallocated Class A network numbers and allocates the "Host Id" portion in a manner analogous to subnetting. The first few bits of the "Host Id" field are used to identify a large organisation or service provider which then suballocates blocks of the remaining bits to their users, which may then

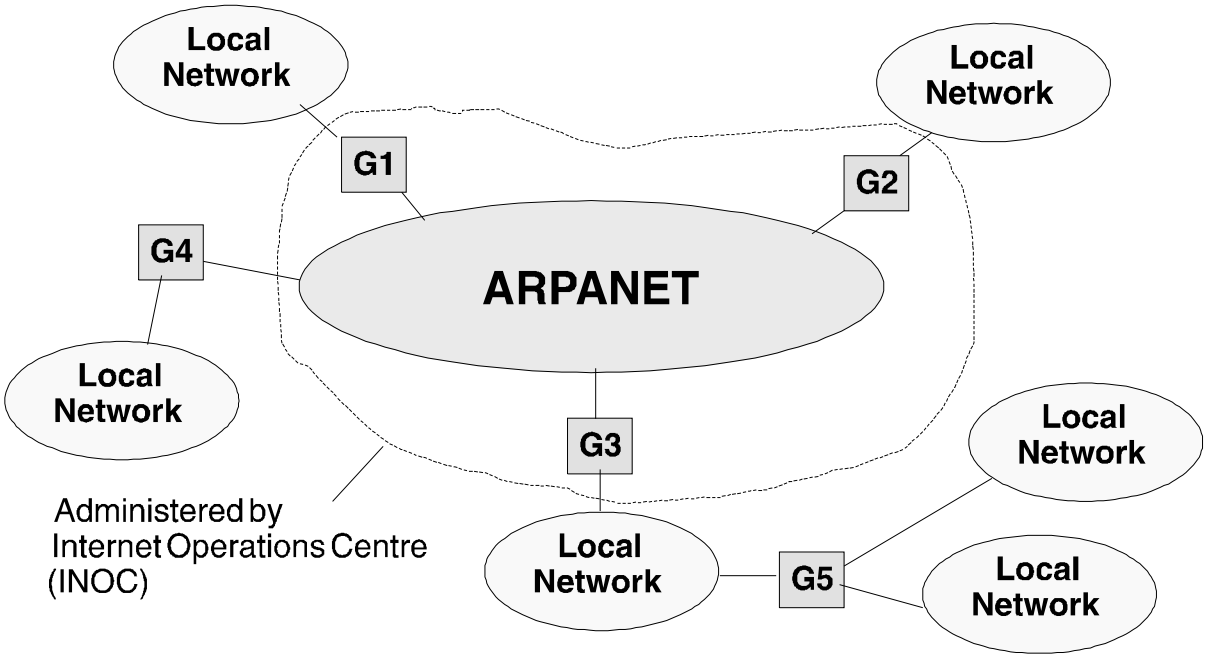

Figure 2 Original Internet Architecture

subnet the remaining bits. CIDR then takes advantage of Route Aggregation principles in routing information exchange protocols such as IDRP to combine routes together so that the routers in one service provider may need only a single entry in their routing tables for routing to all users of another service provider.

3.3 Mobility and the Internet

A simple consequence of Internet Addresses being the addresses of points of attachment rather than End Systems, is that a Host Computer must have a different address for each point of attachment to the Internet. For multi-homed Hosts this means that the Internet Address chosen by another Host for sending packets to it, out of those assigned to each point of attachment, determines the network adapter through which the packet is delivered, and probably the network over which the packet is delivered and the route as well. This is no aid to resilience through multiple points of attachment, as if any of the network adapters fails, in order to use a different one, the sender must be aware of the alternative Internet Addresses, and change to using one that is still available.

For truly mobile systems, the implication of having many different points of attachment to the Internet, and hence Internet Addresses, is that a sender, without additional management protocols, will have great difficulty in determining which point of attachment is in use, and hence which Internet Address to use. An exhaustive search of all known possible points of attachment would seem to be the only possible strategy.

One way of avoiding this problem could be to make it appear as if each mobile system was a separate network. Network numbers are effectively assigned randomly, and dynamic routing protocols could be used to report the new route to such a “network”, every time it attached to a different router. However, this runs up against the problem of overflowing routing tables in core Internet Routers described above, and is not a viable solution. This situation could be avoided if Service Providers to mobile systems employed CIDR techniques to hide all such “mobile networks” from the rest of the Internet. However, CIDR has yet to be widely deployed, and this approach has not been followed for Mobile IP. Also, there would be no obvious way to move between service providers with such a strategy.

Instead, Mobile IP has been developed to require as little change to the existing Internet infra-structure as possible, and techniques have been developed to manage the many different Internet Addresses that a mobile system may have i.e. one for each possible point of attachment, and to permit other Internet Hosts to send packets to mobile systems regardless of where those mobiles are currently attached to the Internet. The strategy described below as Basic Mobile IP, permits communication with mobile systems from all existing Internet attached computers. The second strategy, described below as “Optimised Mobile IP” removes routing inefficiencies inherent in the first approach, but at the expense of requiring additional procedures in Internet Hosts.

3.4 Basic Mobile IP

Figure 3 illustrates the architecture developed for Mobile IP. This introduces two new types of system - the “Home Agent” and the “Foreign Agent”, and uses a technique known as

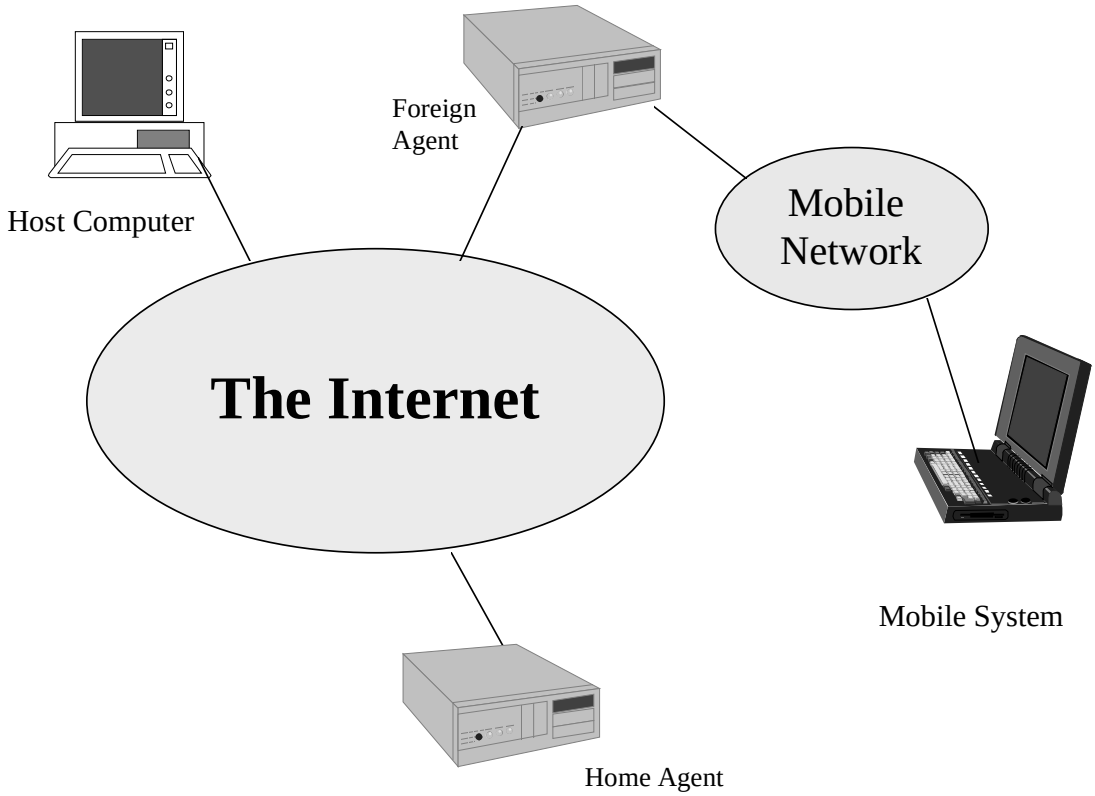

Figure 3 Mobile IP Architecture

encapsulation.

Under Mobile IP. each Mobile Host is assigned a unique “Home Address”. This will be an address on a network associated with a specialised router, which is the Mobile Host’s “Home Agent”. The local routing tables are set up so that packets addressed to the Mobile Host are almost always routed through the Home Agent. The only exception is the special case when the Mobile Host is actually attached to its home network and hence available on its Home Address. In this case, packets may be routed directly to it without passing through the Home Agent.

A Home Agent may be responsible for many Mobile Hosts, and there may be many different Home Agents in the Internet, each supporting a different population of Mobile Hosts.

When another Host wants to send a packet to a Mobile Host, it addresses that packet to the Mobile Host’s Home Address. If the mobile is “at home”, then the packet will be routed

directly to it, otherwise, routing tables local to the Home Address ensure that it will be routed to the “Home Agent”, which must then forward the packet to the mobile’s actual point of attachment, if any.

To be reachable when away from home, a mobile cannot just attach to any point on the Internet, and typically attaches to a point supported by a “Foreign Agent”, that is willing to support the mobile Host’s communications.

When a mobile attaches to a Foreign Agent, the Foreign Agent assigns it a temporary “care-of-address”; this is typically the Internet Address of the Foreign Agent itself. Registration messages are then sent to the “Home Agent” informing it of the care-of-address through which the Mobile Host is now available, and the “Home Agent” is then able to forward packets to the Mobile Host.

When a packet arrives at the Home Agent and addressed to a Mobile Host’s Home Address, that packet cannot just be launched on to a route to the Foreign Agent, as Internet Routers between the Foreign and Home Agents will not in general be aware of Mobile IP procedures, and will just return the packet back to the Home Agent. The Home Agent could replace the Home address in the IP header by the care-of-address. However, when the packet arrived at the Foreign Agent it would then not necessarily have any way of telling to which Mobile Host currently attached to it, the packet was really addressed. This could also interfere which the TCP checksum calculation.

Instead, the Home Agent encapsulates the packet, including its IP header, as the data portion of another IP packet. This IP packet has the Mobile Host’s care-of-address as its destination address.

This encapsulated IP packet may then be successfully routed to the Foreign Agent without any intermediate router having to be aware of Mobile IP procedures. Once it arrives at the Foreign Agent, the packet is decapsulated and the Foreign Agent inspects the original IP Header in order to determine the Home Address to which the packet was originally sent. If this matches the Home Address of any Mobile Hosts currently attached to this Foreign Agent, then the packet is relayed to it; otherwise the packet is discarded.

Packets sent from the Mobile Host to any Host on the Internet do not have to pass through the Home Agent, and are simply routed through the Foreign Agent as normal (non-encapsulated) packets addressed to their intended destination. The source address on such packets is the Mobile Host’s Home Address.

3.4.1 Attaching to a Foreign Agent

A Foreign Agent is a specialised router attached to a Mobile Network, and Mobile Hosts, once attached to the Mobile Network, communicate with it directly over the Mobile Subnetwork.

When a Mobile Host first attaches to a Mobile Network, it must first find out the local subnetwork address of a suitable Foreign Agent and be assigned a care-of-address. This procedure may use network specific procedures. Alternatively, it may use an enhanced version of the ICMP Router Discovery protocol. This is an existing specification which enables Host Computers to dynamically discover routers, and is very similar in function to the ISO 9542 ES-IS protocol. The ICMP Router Discovery protocol message format is extended by Mobile IP to enable Foreign Agents to be distinguished from ordinary routers; to advertise the capabilities of Foreign Agents; and to enumerate the care-of-address(es) supported by the Foreign Agent.

3.4.2 Registration

Once a suitable Foreign Agent has been located, the Mobile Host must register with its Home Agent, informing it of care-of-address that it will now be using. For security reasons this has to be initiated by the Mobile Host and not the Foreign Agent.

Registration is performed by sending a Registration Request datagram to the Home Agent using UDP and relayed by the Foreign Agent. The Registration Request identifies the Mobile Host by its Home Address, announces the care-of-address that it will be using, and proposes a lifetime (in seconds) for the registration. When the Home Agent receives a registration request, it responds with a Registration Reply datagram, again using UDP, confirming the registration and the actual lifetime of the registration.

The Registration Reply is also relayed back via the Foreign Agent, which passes it on to the Mobile Host. The Foreign Agent also responds to a Registration Reply by recording the registration of the Mobile Host and its lifetime. It will then be able to provide forwarding services during the period of the registration.

As UDP is an unreliable transport protocol, registration requests may have to be repeated if a Registration Reply is not received within a given period.

3.4.3 De-registration

De-registration occurs either on the expiration of the registration lifetime or when a Registration Request is received and accepted from a new care-of-address, unless simultaneous mobility bindings have been requested (see 3.4.4 below). A Mobile Host can also de-register without registering a new care-of-address, by sending a Registration Request with a lifetime set to zero.

3.4.4 Multiple Point of Attachment

The Mobile IP Specification can cope with Mobile Hosts concurrently reachable via more than one care-of-address, provided that the Home Agent can support this. In such cases, the Home Agent sends a copy of each packet that it receives and addressed to a Mobile Host, via each currently registered care-of-address. Multiple simultaneous bindings have to be explicitly requested on each Registration Request, if each successive registration is not to replace the preceding one, and a Home Agent may impose a limit on the number of simultaneous bindings that it can accept.

The strategy is profligate in its use of network resources, but useful when a mobile comes into contact with several mobile networks, needs a robust service, and is not sure which mobile network will stay within range and from which it will soon go out of range.

3.4.5 Operation without a Foreign Agent

Although all the preceding discussion has involved the use of a Foreign Agent, the Mobile IP specification also permits operation without a Foreign Agent. This is possible when a Mobile Host is dynamically assigned a unique care-of-address (i.e. one not currently assigned to any other node on that network) when it attaches to a mobile network. For example, this is possible using the Dynamic Host Configuration Protocol (DHCP).

In such cases, the Registration Request is sent direct to the Home Agent, and the Registration Reply is similarly sent direct to the Mobile Host, since the care-of-address uniquely identifies the Mobile Host on the Mobile Network. When the Home Agent forwards packets to the care-of-address, these will be encapsulated as before, and sent to the care-of-address. As this is now the current address of the Mobile Host, it will receive encapsulated packets and must be capable of decapsulating them, verifying that the inner packet is properly addressed to its Home Address, and then handling the packet as normal.

3.4.6 Security

Security is a major problem in Mobile IP. Mobile IP is clearly vulnerable to masquerade and replay attacks and authentication procedures are built into the specification and cannot be considered as an optional add-on. In particular, the registration dialogue has to be protected by digital signatures and non-repeating sequence numbers in order to protect against masquerade and replay.

Mobile Hosts and Home Agents must therefore implement suitable encryption algorithms (MD5 is specified) and Key Management and Distribution Procedures are required.

3.4.7 Mobile Routers

Mobile IP has been designed for Mobile Hosts, but the procedures can be extended to cover the case where an entire “platform” is mobile and comprises several hosts, a local network and a router. In this case, it is the router that is the mobile system (i.e. has a Home Address, registers with a Home Agent, etc.), and the Hosts on board the mobile platform will typically be fixed relative to the router.

The Mobile Router will need to be seen by the Home Agent as an adjacent Router reached over a virtual rather than a real data link. In this situation, the care-of-address registered by the Mobile Router becomes the other end of the virtual data link. Normal routing information may be exchanged between the Mobile Router and the Home Agent, using a Routing Information exchange protocol such as OSPF or IDRP, so that the Mobile Router may keep the Home Agent (as a Router) informed about the Hosts on board the mobile platform and reachable via the Mobile Router.

3.4.8 Congestion Management

Congestion is a major problem for any connectionless internetwork and congestion avoidance procedures are essential if network resources are to be used efficiently and a catastrophic degradation of service is not to be experienced when the network becomes congested. Traditionally, Congestion Avoidance in the Internet has required co-operative “good citizen” behaviour by all Host Computers, by implementing Congestion Avoidance in the TCP implementation.

TCP Congestion Avoidance Procedures require that when the onset of congestion is reported, the TCP implementation “backs off”, that is it decreases its rate of packet transmission by assuming a smaller send credit window than is actually available, and then gradually increases its transmission rate until the send credit window is fully utilised. The back off procedure also applies to retransmissions of already sent packets.

As long as enough Host Computers “Back Off” when congestion is imminent, the load on the network decreases and congestion is avoided.

The onset of congestion is determined either by the need to retransmit a packet, with the assumed reason being that the packet was discarded by an overloaded router, or an explicit report sent back by a router indicating that it is becoming congested (Source Quench). In the former case, it is important that the retransmission timer is set accurately to avoid both false indications of congestion, if set too short, and undetected congestion (and hence the backoff procedures not being applied when they should be), if set too long.

3.4.8.1 Congestion Management and Mobile IP

Mobile IP has two, as yet unsolved, problems with congestion management. The first is that there is a much higher variance in the round trip delay with mobile systems, caused partly by the characteristics of some mobile networks, and also due to changes in path length

when a mobile changes its point of attachment. This will cause problems with the current back-off algorithm due to the greater uncertainty in measuring the round trip delay.

The second is that with mobile IP, packets are also likely to be discarded because a mobile has changed its point of attachment to the Internet. If such discards are also assumed to be due to congestion then the back-off algorithm will be invoked unnecessarily and throughput will suffer. Similarly, packets also likely to be discarded if the mobile network does not provide for local recovery from detected errors, This is because communications errors are much more likely in mobile networks compared with fixed networks. Invoking the back-off algorithm as a result of communications errors will also impact throughput.

To counter these problems, the sending Host Computer probably will need some sort of indication from the network that a mobile changed its point of attachment, and hence the transit delay may undergo a sudden change and packets may be discarded, or that a packet was discarded due to communications errors, rather than just due to congestion. However, getting such an indication is difficult due to encapsulation between Home Agent and Foreign Agent, and it is during this phase of the packet's journey that such problems will arise.

In general, if a router discards a packet, it can return an ICMP packet to the sender reporting the reason for the discard, the IP Header of the discarded packet and the first 64-bits of the data contained in the packet. 64-bits is normally enough information to identify the TCP connection affected by the problem. However, when such a router is along the path between a Home Agent and a Mobile Host, the packet will be encapsulated. The ICMP packet will be returned to the Home Agent, as the sender of the encapsulated packet, and contain only the first 64-bits of the header of the inner packet. This is not enough to include the source or destination address of the inner packet, let alone the TCP connection information.

Because of this problem, it is not readily possible to return to the real sender an indication of packet discard and why it was discarded. The Home Agent may get an ICMP message informing it that an encapsulated packet was discarded. However, if more than one Mobile Host supported by the Home Agent was using the same Foreign Agent then it is not possible to determine which one's packet was affected. In any case, the TCP connection cannot be determined and the Home Agent cannot reconstruct a meaningful ICMP message to return to the original sender.

This is where the current draft for Mobile IP leaves off, with no definite solution to the problem. It is, however, probable that in order to deal with congestion, the Home Agent will have to intelligently monitor the data flows encapsulated by it and predict which ones were the target of ICMP messages using, for example, known information about changes to Mobile Host registrations.

Modified procedures in ordinary Internet Hosts will also be necessary to communicate efficiently with mobile systems, both in changes to the back-off algorithm and in responding to network originated information.

3.5 Optimised Mobile IP

Mobile IP will typically result in sub-optimal routing of packets addressed to mobile systems. This is because such packets will have to be routed via the Home Agent, and this may be a considerable distance from the optimal route between sending Host and the destination mobile. To avoid this problem. a further specification has been developed, which requires additional protocol and support in the sending Host. This specification permits:

1. Host Computers to query a Home Agent as to the current care-of-address of a mobile and hence encapsulate packets and send them directly to the care-of-address without having to pass through the Home Agent.

2. Host Computers to inform sending Hosts of the care-of-address, either in response to an explicit request, or as an informative redirection message, when a packet is relayed through the Home Agent and to a mobile.

3. Foreign Agents to be informed of new care-of-addresses for Mobile Hosts that they had been responsible for and hence to forward packets to the new care-of-address.

4. Foreign Agents to warn sending Hosts when IP packets are received direct from such a Host and the mobile is no longer reachable via the Foreign Agent.

Security is also a very serious issue with this optimisation and considerable additional requirements in support of mobile IP optimisation are due to the need to authenticate the messages that redirect traffic to care-of-addresses. Security is also more costly in this case, as there is a need for a Security Association between each sending Host and the mobile's Home Agent, with the associated cost of key management.

In addition to the cost of security, this optimisation also means that new behaviour is required of Internet Hosts. It cannot be applied to existing systems.

3.6 Discussion of Mobile IP

1) Mobile IP aims to support mobile systems on the existing Internet and enable their communication with existing Host Computers. In this it appears to succeed. However, there have to be compromises, due to the need to enable communication with existing Internet Hosts, and this results in sub-optimal operation.

   - Firstly, routing via Home Agents results in sub-optimal routing away from the direct path between sending Host and Mobile. An optimisation to avoid this has been proposed, but this necessarily involves changes in functionality to the sending Host Computer.

   - Secondly, Congestion Management is also an area in which sub-optimal performance is likely without further modifications to sending Host Computers. Existing implementations communicating with mobiles are likely to enter the back-off algorithm much more often than they should with the consequence of a reduction in throughput.

2) Security is also a significant issue and adds a cost to Mobile IP. It will also cause a problem in optimisation as only Host Computers which include the optimisation extensions and which have a suitable security association (i.e. agreement on encryption algorithms, keys, etc.) can use the optimisations. There is thus a considerable barrier to more optimal routing to mobiles which will probably only be overcome in cases of overriding necessity.

3) Robustness is another issue. If the Home Agent either fails, or becomes isolated from the Internet, then communication with all of its mobiles is lost, even if they have no problem connecting to the Internet. Multiple Home Agents are permitted, but if they are to be geographically dispersed, then a given Mobile must have a different Home Address for each such Home Agent. To allow for robustness by having multiple Home Agents, it would therefore be necessary for a sending Host Computer to have to try each Home Address in turn to find one that worked, or then determining that the mobile is not presently reachable. In itself, this requires further behaviour of ordinary Internet Hosts that is not generally required, but specific to handling mobiles.

4) Utilising multiple concurrent mobile subnetworks is also desirable for robustness and for avoiding short term loss of communications. However, this is an expensive strategy with Mobile IP, given that in such a situation all packets to a given mobile

have to be copied for transmission over every mobile subnetwork. This is itself a consequence of not having any general mechanism for quickly detecting and reporting that a mobile has detached from a mobile subnetwork. There also appears to be no provision for policy based use of different mobile subnetworks, and keeping some available for backup, while not incurring the cost of sending data.

5) Encapsulation is also an added problem in its own right. Packets that were just large enough to go through a network without fragmentation (and packet size is often chosen with such a limit in mind), will be longer when encapsulated and hence may then be fragmented with all the overhead that this implies.

4. Mobility in the ATN

The ATN Internet uses OSI rather than Internet Protocols and, while the OSI CLNP is an evolutionary development from the Internet's IP, the addressing and routing strategy is very different and more amicable to mobility.

OSI CLNP first supports a much larger address space than IP, and this allows for a structuring of the address space that is designed for efficient routing and allocation, rather than a compromise to make best use of a limited address space. More importantly for mobile systems, however, were the original influences on OSI CLNP. These came from manufacturers, such as ICL and DEC, developing distributed systems in a multi-LAN environment. A typical requirement was to enable a process (e.g. a virtual machine) to move from one real system to another without affecting end users.

Such influences led to the development of an addressing plan (NSAP Addressing) that neither addressed ports nor even real systems, but instead addressed entities on systems. Further, such addresses were not relative to networks, but instead were relative to *areas* which comprised several networks and systems. With the routing protocols developed to support this, it was readily possible for an entity addressed by an NSAP Address to be readily mobile within its area without having to change any aspect of its address. Such an entity could be mobile with respect to real systems, or, if the underlying networks allowed systems to readily attach to and detach from them, then real systems could be mobile as well.

As the OSI Routing Protocols were further developed to interconnect on a wide area basis, the mobility that had been permitted within a Routing Area was itself extrapolated to enable Routing Areas within a Routing Domain to be mobile with respect to each other. Similarly, Routing Domains within a given region may also be mobile with respect to each other. Mobility was not a design goal of OSI routing as it was extended to cover wide area internetworking. However, because it was built into the local area routing, the natural extension of OSI routing included mobility support.

The ATN is required to operate on a global basis and many of the requirements placed on it required policy based routing i.e. air-ground subnetwork choice was to be based on policy considerations as well as availability, and sometimes in spite of availability. The need for policy based routing on a large scale implies inter-domain routing, and therefore, the solution adopted, after investigation of the alternatives, was to require each ATN Mobile to be a Routing Domain in its own right. Each such mobile Routing Domain may then be mobile with respect to the ATN fixed systems, which are themselves organised in to fixed, ground based Routing Domains. As both a consequence of and a reason for this decision, the Inter-Domain Routing Protocol (IDRP) was adopted as the routing information exchange protocol between ATN Routing Domains, including Mobile systems.

IDRP does in fact support policy based mobile routing without additional functionality. This is a consequence of not requiring the addresses of adjacent Routing Domains to be related in any way, and by being able to manage dynamic changes in routes to given destinations, including policy based choices between alternative routes and networks. There is no need to resort to subterfuges such as encapsulation to make it work.

IDRP also supports the policy based merging of routes to related destination groups, and this facility, known as Route Aggregation, is essential to the development of scaleable internet architectures. Indeed, this feature of IDRP is necessary to support the Internet's CIDR. However, mobile systems, by their very nature, will not have addresses similar to the systems on the ground to which they are attached to, and cannot usually be grouped together in a manner necessary for Route Aggregation to work. There is thus little or no scope to reduce the number of routes to mobiles distributed around the ATN Internet - an essential feature of scaleability. The ATN is thus vulnerable to the too many routes problem that has already affected the Internet. Furthermore, as routes to mobiles change frequently, the rate of route update is also significant, in turn leading to a significant load on ATN

Routers. The ATN specification has thus been developed to minimise this problem through careful use of routing policy to restrict the scope of route advertisement, and hence to optimise the mobile routing capability inherent in IDRP, but without requiring special procedures on End Systems.

Mobile Routing in the ATN is explained below.

4.1 Mobility in the ATN

As discussed above, the systems onboard an aircraft form a Routing Domain unique to that aircraft and characterised by a single address prefix for all ATSC and AISC systems onboard the aircraft. As an aircraft proceeds on its route, it interconnects with ground based Routing Domains over the various air/ground networks; the actual network used and Routing Domain interconnected with, dependent on the aircraft's actual position, and the airline's routing policy. Routing Information is then exchanged between ground Routing Domains, using IDRP, so that all ground Routing Domains are aware of the current route to that aircraft. This is illustrated in Figure 4.

In this example, there are four ground based Routing Domains RD1 through to RD4. RD1, RD2 and RD3 all support air/ground datalinks, while RD4 depends on the other three for air/ground communications. For the purposes of this example, it is assumed that the aircraft currently has communications over air/ground datalinks with both RD2 and RD3.

Using IDRP, both RD2 and RD3 advertise a route to the aircraft's systems, to RD4. RD4 chooses between these two available routes using its own Routing Policy, which might, for example, favour the route through RD3. Similarly, the aircraft's router must choose between the routes to RD4 offered by RD2 and RD3. It need not make the same choice as RD4. In both cases, different routes may be chosen in support of different applications.

As the aircraft continues on its journey, it may lose communication with RD3. For example, it goes out of range of the VHF datalink it was using to communicate with RD3. RD3 informs RD4 of this situation by issuing the appropriate IDRP protocol to withdraw the route, and RD4 now changes to using the route offered by RD2, as it is now the only route to the aircraft. The aircraft's router also recognises the loss of communication with RD3 and must now route all traffic via RD2.

Further on the journey, the aircraft comes into contact with an air/ground datalink offering communication with RD1. A datalink is established and routing information exchanged. RD1 now advertises the new route to the aircraft, to RD4. RD4 now once again has two routes to the aircraft and must make a choice between them using its local routing policy rules. It might, for example, now prefer the route through RD1, in which case all data to the aircraft is now routed via RD1. The router in the aircraft also goes through a similar decision process.

While the topology of the ATN ground environment is much more complex than the above example, this is essentially how mobile communications is implemented by the ATN.

4.2 Containing the Impact of Mobility

While the principles of mobile routing outlined above are straightforward they are not scaleable using the existing IDRP mechanisms associated with Route Aggregation and RDCs. The problem is that even if an aircraft is given an address prefix similar to the address prefixes that characterise the ground Routing Domains at the start of its journey, such a similarity is unlikely to be maintained for the duration of the flight. Route Aggregation possibilities are thus very limited.

Instead, an alternative mechanism has been developed to permit mobility within a scaleable Internet architecture, building on two concepts: the ATN Island, and the “Home” domain (see 4.4 below). In addition, the ATN Addressing Plan specifies a common address prefix for all aircraft and, subordinate to that address prefix, specifies a unique address prefix for the aircraft belonging to each airline, and the General Aviation Aircraft of each country.

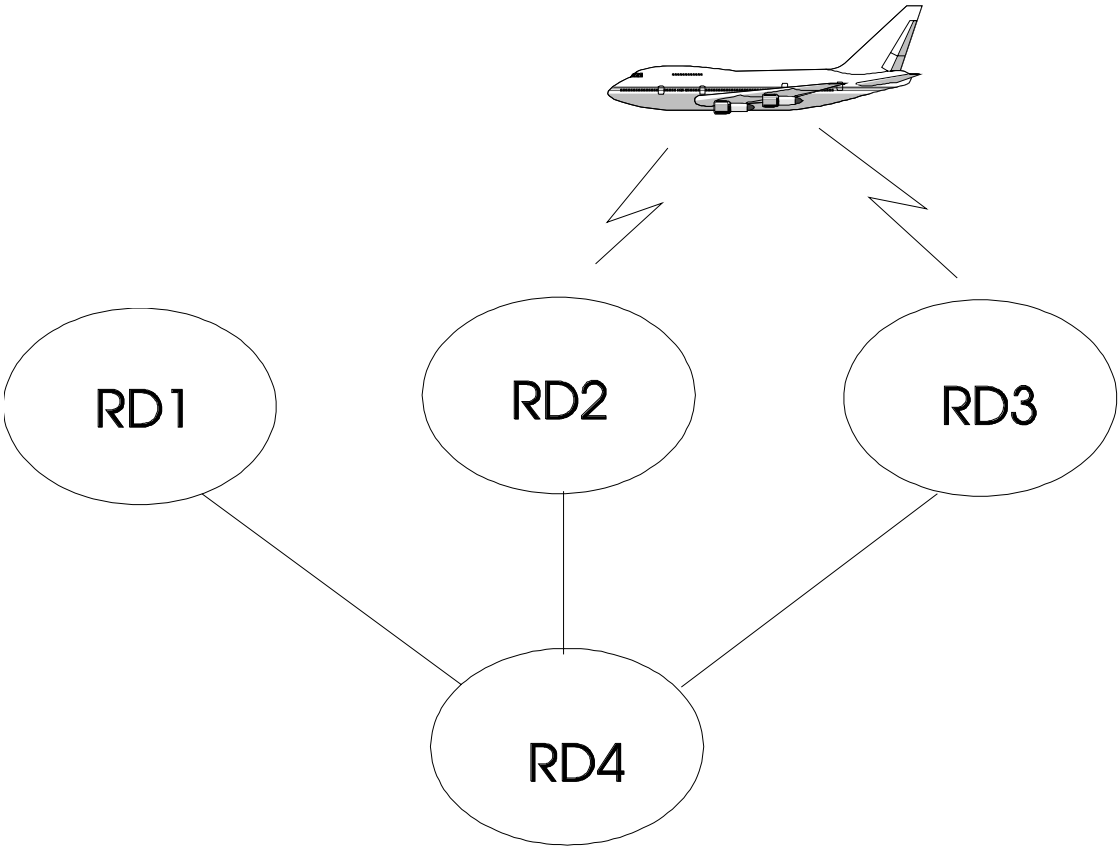

Figure 4 Mobile Routing Example

4.3 Routing to Mobiles within an ATN Island

An ATN Island is simply an ATN region comprising a number of Routing Domains, some of which support air/ground datalinks. These Routing Domains form a Routing Domain Confederation (RDC)[1], as illustrated in Figure 5, and an ATN Island is essentially an RDC in which certain Routing Policy rules are followed. All ATN Routing Domains that have air/ground datalink are members of an ATN Island and, although most ATN Routing Domains which do not have air/ground datalink capability will also be members of ATN Islands, they do not have to be, but then cannot have access to routes to aircraft if they are not a member of an ATN Island RDC. Routes to destinations in ground based Routing Domains will be exchanged by ATN Routing Domains, both within an Island and between Islands. However, this is outside of the context of the ATN Island. The ATN island exists to support routing to mobiles and only applies to this case.

[1] An RDC is simply a group of Routing Domains. Although not formally required to relate to addressing, a typical use for an RDC is to group together all RDs with a common address prefix.

Within each ATN Island, at least one Routing Domain forms the Island's *backbone*. This is another RDC comprising all backbone Routing Domains in the same ATN Island.

Within the ATN Island, the Backbone RDC provides a default route to *all aircraft*, as illustrated in Figure 5, this is advertised to all other Routing Domains within the Island as a route to the common address prefix for all aircraft.

Routing Domains with routes to aircraft then have a simple routing policy rule to determine to which adjacent Routing Domain they must advertise such a route[2]. This is the Routing Domain currently advertising the preferred route to *all aircraft*. This will be a backbone Routing Domain if such a Routing Domain is adjacent, otherwise it will be a Routing Domain that provides a route to the backbone. Either way the impact of such a policy rule is that the Backbone RDC is always informed about routes to all aircraft currently reachable via datalinks available to the Island's Routing Domains, and can thus act as default route providers for packets addressed to airborne systems.

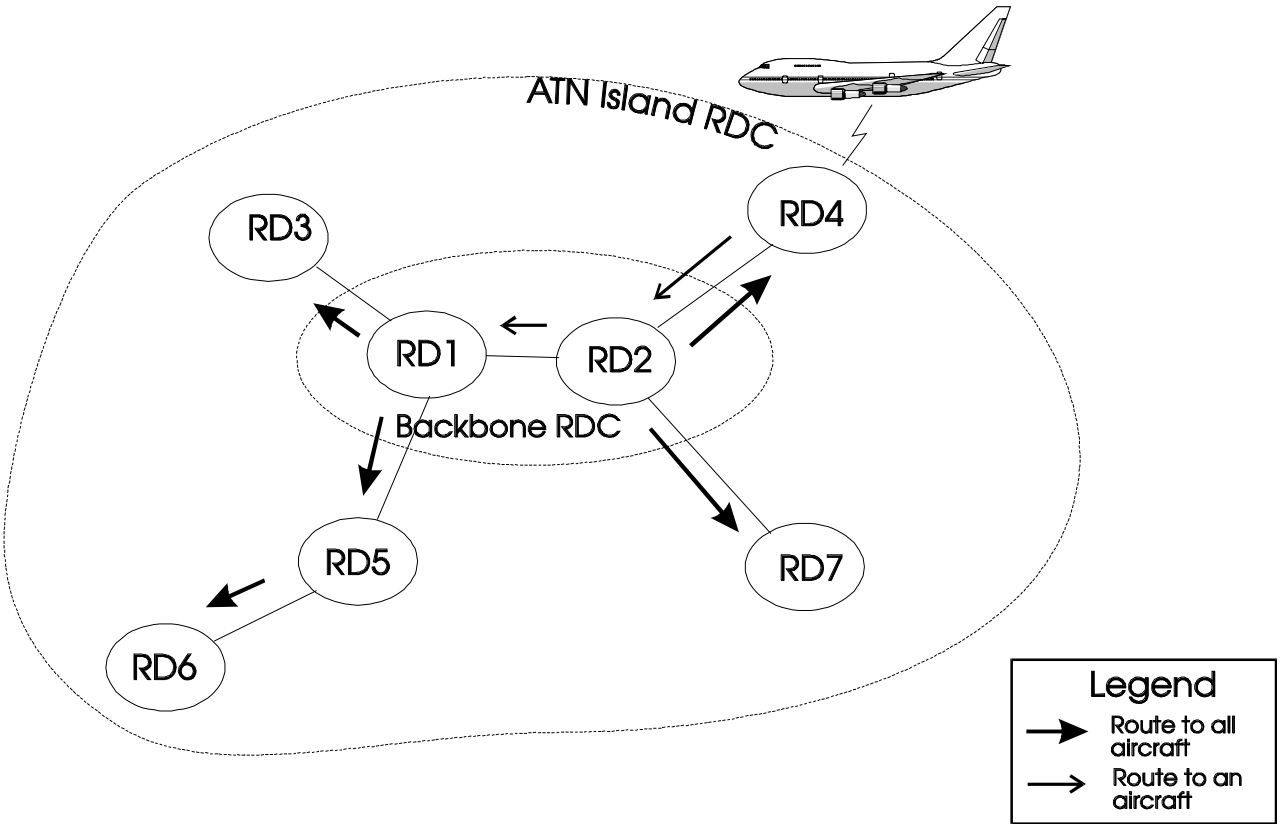

Figure 5 Mobile Routing Within an ATN Island

Routing Domains off the backbone also have a simple routing decision to make when they need to route a packet to a given aircraft. It is routed along the explicit route to the aircraft if it is known by them, or on the default route to all aircraft via the backbone, otherwise. Routing with IDRP always prefers routes with the longest matching address prefix. Therefore, the default route to all aircraft is always a shorter prefix of that for an explicit route to an aircraft, and this routing strategy happens automatically without any special provisions.

[2] A route to an aircraft is readily identifiable from the destination address prefix, as all address prefixes that characterise an aircraft Routing Domain descend from a unique address prefix.

The above is not the only policy rule that can apply to routes to aircraft. Routes to aircraft can be advertised to any other Routing Domain within the Island, provided that a policy rule is set up to allow this. This may be because there is a known communication requirement which makes bypassing the backbone desirable, or because it is desirable to provide a second (hot standby) route to aircraft from the backbone. The architecture accommodates these requirements. The only limitation on this is that imposed by the overhead of supporting routes to mobiles.

Within the Backbone RDC, all Routing Domains must exchange all routes to aircraft, which are advertised to them, they are then able to act as default routers to any aircraft currently in communication with the ATN Island. However, because the backbone routers need to know routes to all such aircraft, their capacity places a limit on the number of aircraft that can be handled by an ATN Island and hence on the effective size of the Island.

The ATN Island is only the first part of achieving a scaleable routing architecture for mobile routing. Its true benefit is to focus the overhead of handling the potentially large number of routes to aircraft on a few specialised routers in the backbone. Off the backbone, a Routing Domain with an air/ground datalink needs only the capacity to handle the aircraft supported by its datalink, and there is a similar impact on Routing Domains that are Transit Routing Domains providing a route between the backbone and an air/ground datalink equipped Routing Domain. For all other Routing Domains on the Island, there is no impact on routing overhead due to aircraft.

In the absence of a backbone, all routers within the Island would need to be explicitly informed with a separate route to each aircraft, if they were to be able to route to any aircraft currently in contact with the Island. This is because there is very little probability of route aggregation with routes to aircraft.

4.4 Routing to Mobiles between ATN Islands

ATN Islands can be set up such that their geographical spread matches Air Traffic Control communication requirements and, for ATC purposes, there may not be a requirement to provide inter-Island communications in respect of aircraft. However, airline operational requirements are perceived to require this, and hence the mobile routing concept is developed to provide a greater level of scaleability.

The mechanism used to achieve this derives from the concept of the “Home” domain.

Aircraft for which inter-Island communications are required must have a “Home” domain, which is a Routing Domain in an ATN Island. This “home” need not be in either the ATN Island through which the aircraft is currently reachable, or in the ATN Island with which communication is required. The role of the “Home” domain is to advertise a default route to all the aircraft belonging to an airline, or the General Aviation aircraft of a given country of registration. This default route is advertised to all other ATN Island’s backbone routers.

The operation of the “Home” domain is illustrated in Figure 6. In this example, ATN1 is the ATN Island acting as the “Home” for all aircraft belonging the same as airline as the aircraft illustrated as currently reachable via ATN4. ATN1 advertises the default route to all such aircraft to all Islands in which it is in contact and, depending on local policy this route may be re-advertised to other Islands. In the figure, ATN3 re-advertises the default route on to ATN4.

The backbone routers of an ATN Island have a simple policy rule to implement for each explicit route to an aircraft that they have available. If a default route to all the aircraft in the

aircraft's airline or country of registration exists[3] then the actual route to the aircraft is advertised to the Routing Domain advertising that default route. Otherwise, the explicit route is not advertised outside of the Island. In Figure 6, the route to the aircraft is first advertised by ATN4 to ATN3 and then re-advertised to ATN1. In each case, the same policy rule is applied.

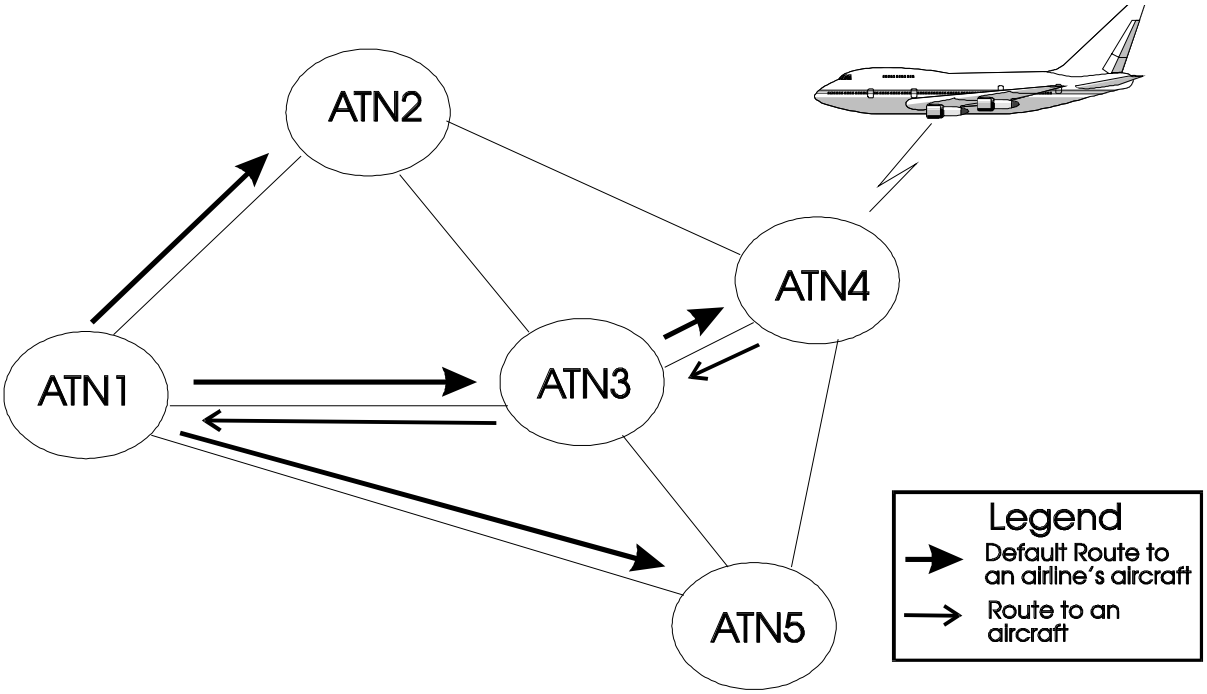

Figure 6 Inter-Island Routing

The impact of this rule is that the "Home" is always kept aware of routes to all of "its" aircraft. As it is also providing the default route to such aircraft, routers on other ATN Islands (e.g. ATN2) that have packets to route to one of that "Home's" aircraft will by default send those packets to the "Home" Routing Domain (ATN1), where the actual route to the aircraft is known, and thus the packet can be successfully routed to the destination aircraft (via ATN3 and ATN4).

In the above example, this is clearly non-optimal as ATN4 can be reached directly from ATN2. However, the loss of optimal routing is acceptable as, otherwise a scaleable architecture could not have been developed.

The impact of this strategy on routing overhead, is that an ATN Island backbone has to be capable of handling routes to all aircraft currently in contact with the Island, and all aircraft for which it is the "Home". Thus, and assuming that all ATN Islands are fully interconnected, if there are at most 'n' aircraft in contact with the Island, and the Island is "Home" to 'm' aircraft then:

n + m < "maximum number of routes to mobiles that can be handled by a backbone router"

has to be true.

[3] Such a route is generated by the "Home" Domain , and is readily identifiable from the destination address prefix, as all address prefixes that characterise an aircraft belonging to the same airline descend from a unique address prefix.

However, this limit is independent of the total number of ATN Islands or the total number of aircraft. It is thus possible to add more ATN Islands, or aircraft belonging to airlines whose "Homes" are on other Islands, without affecting this limit. The routing architecture thus allows for a much larger number of mobile systems than that permitted by a single ATN Island.

4.5 Security

Routing Information is exchanged using IDRP between adjacent Routing Domains. Each Routing Domain (i.e. the operating administration or organisation) takes on responsibility for ensuring the proper delivery of data passed to it along the routes that it advertises. Assurance of the validity of routing information received is a matter for the local Security Policy. IDRP provides mechanisms for the continuous authentication of all data exchanged providing protection from masquerade and replay. These facilities are available when required.

Currently, these security mechanisms are not required for use over air-ground data links, and only a checksum protecting against communications errors is used.

4.6 Congestion Management

Traditionally, Congestion Management procedures in CLNP internets has been very similar to those employed in IP internets. When extended to mobile communications, the following problems are clearly in common:

1. Measured round trip delay may change suddenly when a mobile changes its point of attachment to the internet.

2. Packets may be discarded when a mobile changes its point of attachment and if such discards are assumed to be the result of congestion, the back-off algorithm may be used unnecessarily, thereby reducing performance.

However, the ATN requires that all air-ground data links use reliable communications protocols and therefore there is no increased risk of packets being lost on such data links, than on ground data links. Furthermore, the ATN mobile routing strategy does not require the use of encapsulation. Therefore, Error PDU information reporting packet loss due to changes of a mobile's point of attachment can be readily returned to a packet's sender.

In an ATN scenario, the time between an individual mobile changing its point of attachment is typically large (e.g. 30 minutes for Mode S, and much longer for satellite), the effect on throughput that results from changes in a mobile's point of attachment is therefore not great and unmodified back-off procedures may be satisfactory for the ATN. If it does prove necessary for sending systems to react to a mobile's changed point of attachment, then the procedures for indicating this are clearly straightforward and are not subject to the problems in Mobile IP than result from encapsulation.

4.7 Discussion

1) The ATN Mobile Routing Concept optimises the mobile routing capability inherent in OSI Addressing and Routing in order to support and provide an internet that meets the operational requirements of aeronautical applications. The optimisation is designed to minimise the impact of changing routes and to provide a degree of scaleability. However, this is at a cost of sub-optimal routing.

   - This is because a packet may have to visit a "Home" or an ATN Island Backbone before being routed to the destination aircraft. However, this

diversion is only necessary when explicit routing information is not known locally and, in most cases a packet will follow a near optimal path, diverting to a “Home” or “Backbone” only until explicit routing information is found. This will often be before the “Home” or “Backbone” is actually reached.

- Like Mobile IP, congestion management may also result in sub-optimal performance. However, this is likely to be much less of an issue than with Mobile IP. Firstly, all ATN air-ground networks are required to be reliable. A higher rate of packet loss than in ground networks is therefore unlikely. Secondly, the time between mobile network attachments change is also likely to be much longer than is envisaged with some implementations of Mobile IP (e.g. with cellular radio). The unnecessary invocation of the back-off procedures, which is the cause of sub-optimal performance is therefore likely to be only an occasional event in the ATN, rather than a regular event, and hence will not have that much of an impact on overall performance. As encapsulation is not a feature of the ATN, mechanisms for alerting a sender that packet discard is due to a mobile changing its point of attachment rather than congestion, are straightforward to implement in the ATN, should they be needed. This is in contrast to the problems that Mobile IP has in this area.

2) Mechanisms exist in ATN Mobile Routing to protect against masquerade and replay attacks when exchanging routing information. Unlike the Internet, serious consideration to their use has not been given. This is an area which should be perhaps be subject to review.

3) Robustness in the sense of providing high availability, especially to safety related applications, is a major design goal of the ATN. Priority based mechanisms, which are not a feature of Mobile IP, are used to ensure that scarce resources can be pre-empted by safety related applications, and IDRP explicitly supports high availability by managing multiple alternative routes to the same destination. However, unlike Mobile IP, IDRP does not simply copy packets over every available route. Instead, IDRP conserves network resources by first maintaining information on all available routes, but then dynamically choosing the “best one” for each packet based on policy requirements and performance considerations.

4) In the ATN, routing policy may be determined by local requirements (i.e. by the manager of a router) and by application requirements, indicated on each packet. When multiple routes are available (e.g. over different air-ground subnetworks), packets corresponding to different applications can be routed over different air-ground subnetworks to the same aircraft.