Title: Tunnelled Signalling for the Support of Mobile ATM

Source: John Porter, Damian Gilmurray
Olivetti Research Limited
24a Trumpington Street
Cambridge CB2 1QA
United Kingdom

Phone: +44 1223 343000 Fax: +44 1223 313542
Email: {jporter, dgilmurray}@orl.co.uk

Date: December 2-6, 1996
Vancouver, B.C., Canada

Distribution: WATM

Notice: This contribution has been prepared to assist the ATM Forum. It is offered for discussion and is not a binding proposal on Olivetti Research Limited. Specifically Olivetti Research Limited reserves the right to add, amend or withdraw any or all statements contained herein.

Abstract: This contribution proposes a solution to the problem of supporting mobile ATM devices and is in response to the request for technical proposals made in [1]. The solution described uses tunnelled signalling in combination with a location service to perform location management for mobile ATM devices.

1 Introduction

A number of contributions have proposed solutions to the problem of location management for mobile ATM devices [2-4]. These solutions may generally be categorised into either mobile PNNI schemes where the routing mechanisms of PNNI are extended to cope with mobility or location register schemes where location management is performed outside PNNI. The solution proposed here falls into the latter category.

The solution to location management for mobile ATM has a number of requirements.

- It should be scaleable
  The solution should scale to support large numbers of mobiles where there is possibly rapid mobility between access points. It should work over an arbitrarily large internetwork which involves both private and public ATM networks.

- It should support hosts and networks with no mobility enhancements
  Unmodified hosts and networks should operate transparently with those with mobility enhancements. Furthermore the modifications to existing signalling and routing protocols should be minimised.

- There should be efficient routing of virtual connections
  Virtual connections to mobile ATM devices must be routed on a reasonably optimal path. This is especially true in the wide area where connections traversing the public ATM network will be subject to billing. However it is more important for the system to function adequately with legacy networks and hosts than for the routing to be optimal.

- Management overhead should be minimised
  The mobility of a large number of mobiles should not overload the ATM network with management messaging. The effect of small-scale mobility of mobiles in the local area

should be isolated from the wide area[5]. Furthermore, where there are protocol exchanges involving mobile entities, intermediate switches should be involved in the processing of these messages.

The solution described here proposes the use of *tunnelled signalling* in combination with a location service to manage the mobility of ATM devices. The scheme is applicable to both a scenario in which the wireless link is to a mobile terminal and one in which the link is to a mobile. Most importantly it can operate with no changes to signalling protocols and therefore work with existing and future systems.

2 Architecture

2.1 Addressing

In order to make use of existing PNNI routing protocols this scheme proposes the use of a *Mobile Home Address* (MHA) and a *Mobile Foreign Address* (MFA) to track and locate mobile ATM devices as in [2][3].

A mobile is assumed to originate from a particular network termed its *Home Network*. Services within this network have administrative responsibility for the mobile and maintain information such as the current location of the mobile and security details for authentication services.

When a mobile registers in a network other than its Home Network this network is termed its *Foreign Network*. Services within the Foreign Network are responsible for managing the small scale mobility of the mobile within this network and for registering the current location of the mobile.

An MHA, specifying the Home Network, is allocated to the mobile which stores it in non volatile memory. A possible mechanism for allocating this address is to derive it from the network prefix of the Home Network and the MAC address of the mobile. The MAC address of a mobile is a 48-bit globally unique IEEE MAC address as is suggested for use as the End System Identifier (ESI) in UNI 4.0 [6]. Endpoints which wish to establish a connection with a mobile device use the MHA of the mobile for the called party number in the SETUP request. Similarly mobile endpoints which wish to establish a connection use their MHA for the calling party number in the SETUP request.

It must be possible for a mobile-enabled switch to determine whether a called party number in a SETUP request refers to a mobile. There are two possible approaches: either the address is specified in a table of mobile addresses or the address space is explicitly partitioned. A table-based approach is considered to have a serious performance penalty and therefore a partitioning of the address space is considered necessary.

When a mobile registers in a foreign network it is allocated an MFA by a service in that network. This address may either indicate a switch or an access point in the network or may be derived from the network prefix of the Foreign Network and the MAC address of the mobile.

The dynamic binding of MFA to MHA means that a relatively static binding between ATM endpoints and ATM addresses can be assumed for ATM name server functionality [8]. The view taken by PNNI that the ATM address hierarchy reflects the network topology can also be extended to mobile endpoints.

2.2 Location Service

As has been proposed in other contributions, a Location Service manages the mapping between MHAs and MFAs. The implementation of this Location Service will logically consist of a hierarchy of location registers. The functionality of the Location Service will include services provided in both the Home Network and the Foreign Network of the mobile. These services are supported by location registers respectively termed the Home Location Register (HLR) and the Visitor Location Register (VLR).

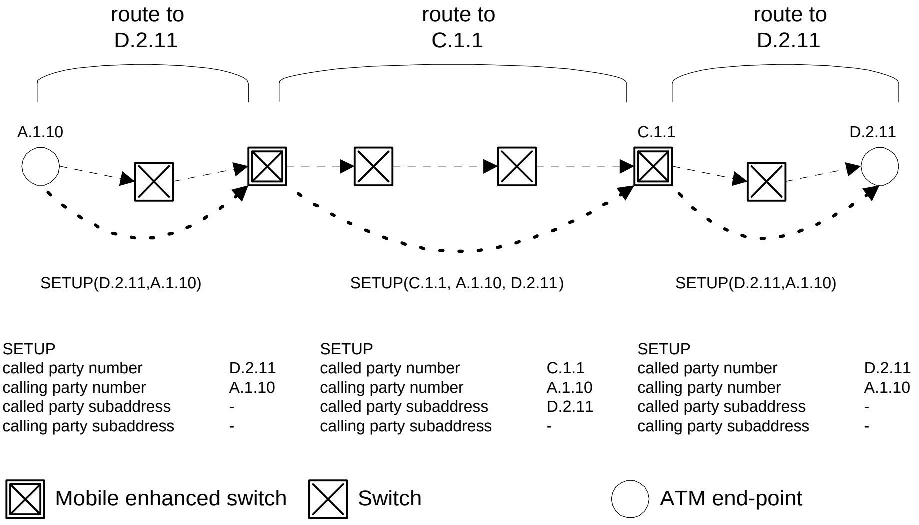
The Location Service protocol should be independent of PNNI and UNI in order to satisfy the scaleability requirement. It can then run efficiently over any ATM network regardless of the underlying protocols and imposes no mobility requirements on those protocols.

The HLR for a mobile is the service at the mobile's Home Network which is the authoritative and fallback location for the mapping from the MHA to its MFA. The HLR can also be used to authenticate the mobile when it is registered in Foreign Networks. Further value-added services such as paging may also be provided by the HLR.

When a mobile registers at an access point in a foreign network using its MHA, the access point contacts the Location Service. The Visitor Location Register (VLR) allocates an MFA to the mobile and caches the mapping from the MHA to this MFA. The Location Service then communicates this mapping through the Location Service hierarchy back to the HLR for the mobile.

2.3 Tunnelling

Tunnelling is a term used to describe the encapsulation of an endpoint address in a message routed via an intermediate address, the *tunnel address*. In the IP Mobility Support RFC [7] tunnelling is used to route datagrams to the current location of mobile IP devices. In this contribution, tunnelling is used for SETUP requests. SETUP requests for the endpoint address are routed via the intermediate *tunnel address* after which the signalling message reverts to the use of the original endpoint address. A simple example of tunnelling is illustrated in Figure 1. We propose that this mechanism be used to support routing SETUP requests for mobile endpoints and networks.



SETUP	
called party number	D.2.11
calling party number	A.1.10
called party subaddress	-
calling party subaddress	-

SETUP	
called party number	C.1.1
calling party number	A.1.10
called party subaddress	D.2.11
calling party subaddress	-

SETUP	
called party number	D.2.11
calling party number	A.1.10
called party subaddress	-
calling party subaddress	-

Figure 1: Example of simple tunnelling

2.4 Tunnelling Implementation

The implementation of tunnelling, as described, requires functionality which enables the encapsulation of the destination address in the connection SETUP request and the reconstruction of the original connection SETUP request at the tunnel exit. This can either be by explicit encapsulation of the destination address within the tunnelled request, or by implicit recovery of the address based on the addresses in the request.

2.4.1 MHA Encapsulation

A mechanism to support explicit tunnelling is already specified in UNI3.0/3.1/4.0 to route connections between private ATM endpoints identified by NSAP-format ATM addresses across a public network supporting E.164 ATM addresses. At the ingress UNI to the public network the private ATM addresses are encapsulated in the Called Party Subaddress and Calling Party Subaddress information elements of a SETUP request. The E.164 gateway addresses of the two private networks are substituted as the new Calling Party Number and Called Party Number information elements. At the egress UNI from the public network, the private ATM calling and called party addresses are extracted from the Subaddress information elements and are used to forward the SETUP request with the original called and calling party private ATM addresses.

In UNI4.0 and PNNI1.0 multiple called party subaddress information elements can be included in a SETUP request. A subaddress information element can therefore be used to transport the MHA in a tunnelled SETUP request where the called party number is the MFA. This is the preferred approach to encapsulation as it is consistent with the current function for this Information Element.

The *Generic Identifier Transport* in UNI 4.0 / PNNI 1.0 is an end-to-end information element. As has been suggested in [3], this could be used to carry the MHA in a tunnelled SETUP request where the called party number is the MFA.

If neither of these approaches are applicable (neither are possible in UNI 3.0/3.1) then a fallback solution is to use *Implicit Tunnelling*. This can only apply where there is a one-to-one mapping between MHA and MFA. If this is the case then MHA can be recovered at the exit of a tunnel with a reverse mapping based on the MFA.

2.4.2 MHA to MFA Translation

A tunnel is entered at the first mobile-enabled switch encountered by the SETUP request as it is forwarded from the calling party towards the MHA. For optimal routing the mobile-enabled switch should be as near to the calling party as possible. A practical solution is to have mobility functionality in the gateway switch between the public and private network. The worst-case scenario is one in which there are no mobile-enabled switches en route to the mobile’s Home Network. In this situation a mobile-enabled switch in the Home Network would perform the tunnelling of the SETUP request to the mobile’s Foreign Network. This architecture allows for a limited initial deployment of mobility enhancements at the cost of sub-optimal routing with the option of progressive improvement.

2.4.3 MFA to MHA Translation

A tunnel is exited either at a mobile-enabled switch or the access point for the mobile. The precise location of the exit of a tunnel is dependent on the handoff model.

There are two main proposals for managing the handoff of connections as a mobile moves between access points. The first model, commonly referred to as the *Path Rerouting Model*, involves rerouting a mobile’s connections from one access point to another via a crossover or anchor switch. In practice the switch may either be a true ATM switch or an access point. The second model, the *Path Extension Model*, involves extending the connections on handoff from one access point to the next.

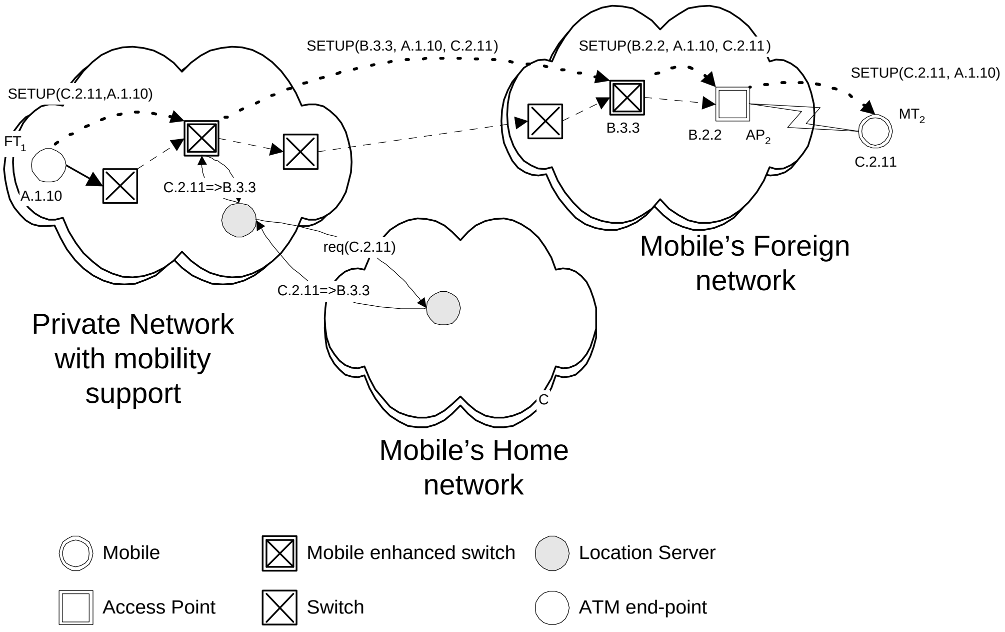
In the path rerouting model the MFA is associated with an anchor switch where the tunnel terminates. Connections are then routed to the appropriate access point using tunnelled SETUP requests where the called party number is the address of this access point.

In the path extension model, the MFA is associated with an access point. On handoff, the MFA will either migrate or be reassigned from the old access point to the new access point. Existing connections at the old access point are extended to the new access point using tunnelled SETUP requests where the called party number is the address of this new access point. Until the MFA address migration or reassignment has taken effect, new SETUP requests will continue to arrive at the old access point. These SETUP requests will then be tunnelled through the access points in the path until they arrive at the mobile's current access point. The migration or reassignment of the MFA places no requirements on the speed of PNNI routing updates as tunnelling bypasses this routing.

Rebinding MFA to MHA requires that the location service be updated frequently. Migration of MFA between access points requires the localised routing to be modified to reflect the new topology. Selection of one or other scheme depends on the tradeoff between Location Service updates and PNNI routing updates.

2.5 Tunnelling to Support Mobile Terminals

2.5.1 Fixed Terminal(FT) to Mobile Terminal(MT)

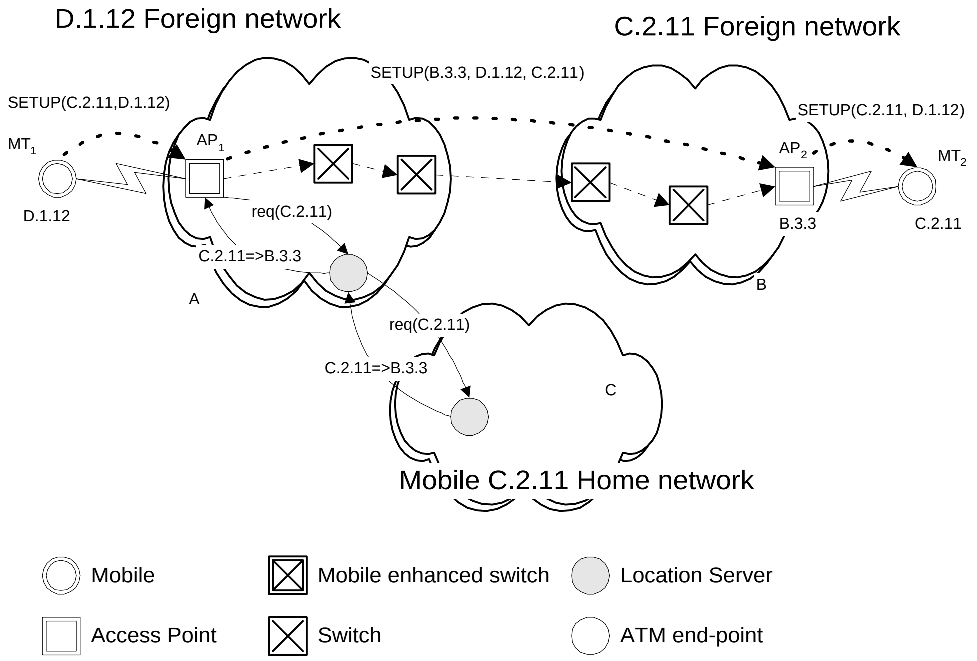


In this example, a connection is originated by FT_1 with ATM endpoint address A.1.10 for mobile MT_2 with MHA C.2.11. The source network is mobile-enabled and the mobile is supported by an anchor switch in its Foreign Network. When the mobile was initially registered at AP_2 the VLR allocated MFA B.3.3 as the anchor switch for the mobile.

- FT_1 generates a SETUP request specifying A.1.10 as the calling party number and MHA C.2.11 as the called party number.
- The SETUP request is routed via a mobile-enabled switch in the source network. The mobile-enabled switch recognises that the called party number is that of a mobile and performs a location request on that address.
- The Location Service returns the MFA B.3.3 for the mobile which in this case is the endpoint address of the anchor switch.
- The called party number of the SETUP request is now replaced with the MFA and the MHA is encapsulated.

- The SETUP request is routed to the anchor switch in the Foreign Network using standard routing protocols based on the MFA.
- At the anchor switch the original called party number is recovered and the SETUP request is tunnelled to the appropriate access point endpoint address.
- The access point receives the tunnelled message and forwards the original SETUP request to the mobile.

2.5.1 MT to MT



In this example a connection is originated from calling mobile MT_1 and destined for mobile MT_2. The mobiles themselves only use their respective MHAs, MHA_1 D.1.12 and MHA_2 C.2.11. Access points are assumed to have Location Service functionality and in this case no mobile-enabled switches are necessary. There are no changes to the signalling protocols.

- Mobile MT_1 originates a SETUP request specifying MHA_1 as the calling party number and MHA_2 as the called party number.
- The source Access Point AP_1 detects that MHA_2 is a mobile address and makes a location request to the Location Service. (For illustrative purposes the VLR is shown forwarding the request to the HLR although in practice the Location Service is likely to have the MHA-to-MFA mapping cached.) The Location Service returns MFA_2 which in this case corresponds to the destination access point B.3.3.
- AP_1 replaces the called party number in the SETUP request with MFA_2 and encapsulates the MHA_2.
- The SETUP request is now routed based on MFA_2 to the destination access point.
- AP_2 now regenerates the original SETUP request by replacing the called party number with MHA_2.
- The VC is completed when the CONNECT message returns along the prototype VC.

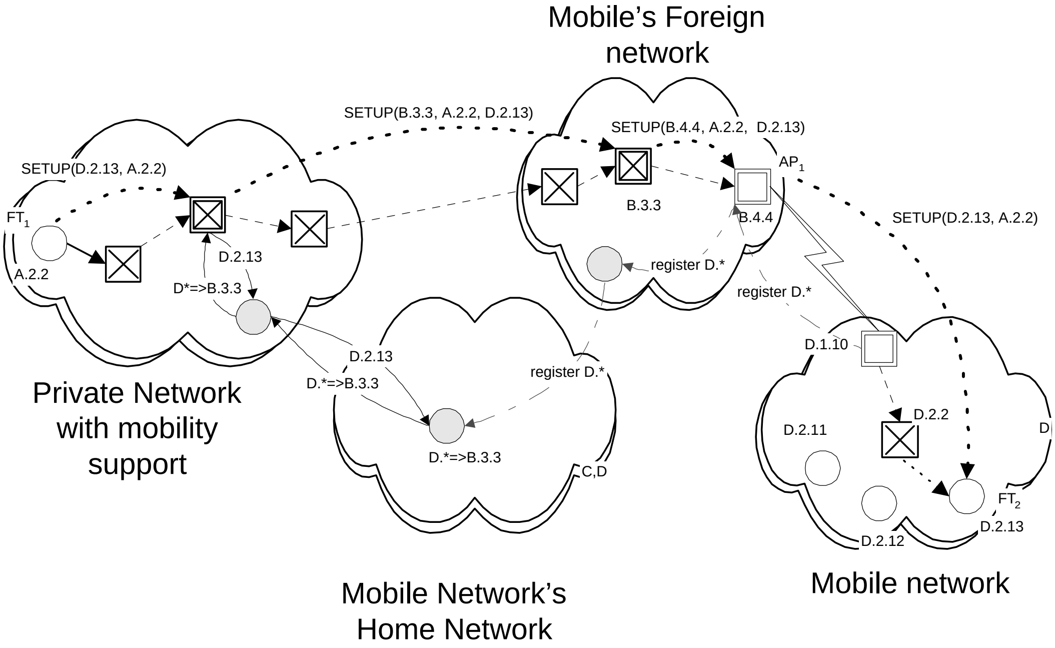
2.6 Tunnelling to Support Mobile Networks

The discussion so far has been focused on the mobile endpoints scenario. Tunnelled signalling is most effective for the location management of mobile or moving ATM networks where the wireless link is supporting multiple ATM endpoints.

In a mobile ATM network, such as a mobile multi-user platform, many ATM devices including switches and endpoints are collectively mobile. To avoid the management overhead of registering a separate MHA-to-MFA mapping for each ATM device in the mobile network, all the devices in the mobile network share an MHA prefix.

When the wireless access point of a mobile network registers at a network, the VLR of the network allocates a single MFA address to the mobile network. The Location Service maintains a mapping from the mobile network's MHA prefix to this MFA. This Network prefix is then used as a mask by which any address within the mobile network can be tunnelled via the same MFA.

2.6.1 FT to FT in mobile network

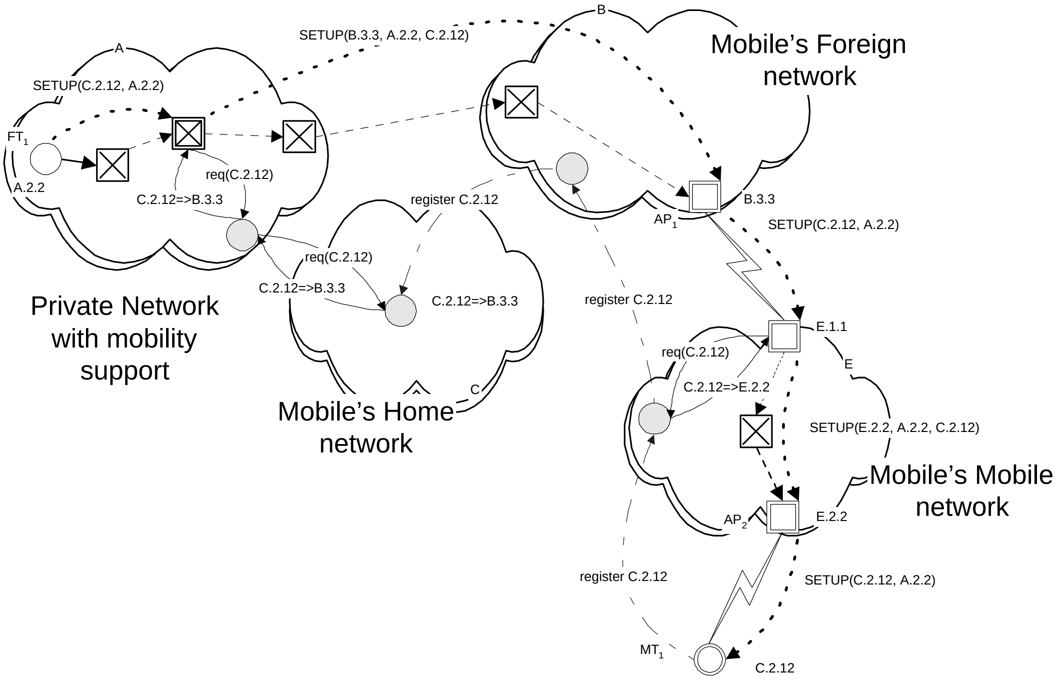


In this example a mobile network is supported. There are assumed to be terminals which are fixed with respect to the mobile network. In this case the Location Service can manage the mobile network as a whole. All endpoints within the mobile network have the same network prefix D which identifies them as mobile. Non mobile-enabled switches will by default route connections to the 'Home Network' of D which is C.

The mobile access point AP$_1$ registers the mobile network using its network prefix D. The Location Service now 'wild cards' any addresses with that prefix and assumes that they are all contacted via the same MFA. The Location Service and any VLRs only need a single entry for all endpoints within the mobile network

The tunnelling procedure is now identical to that for a single mobile endpoint. The only difference is that the Location Service only needs to match the network prefix for the mobile network.

2.6.1 FT to MT in mobile network



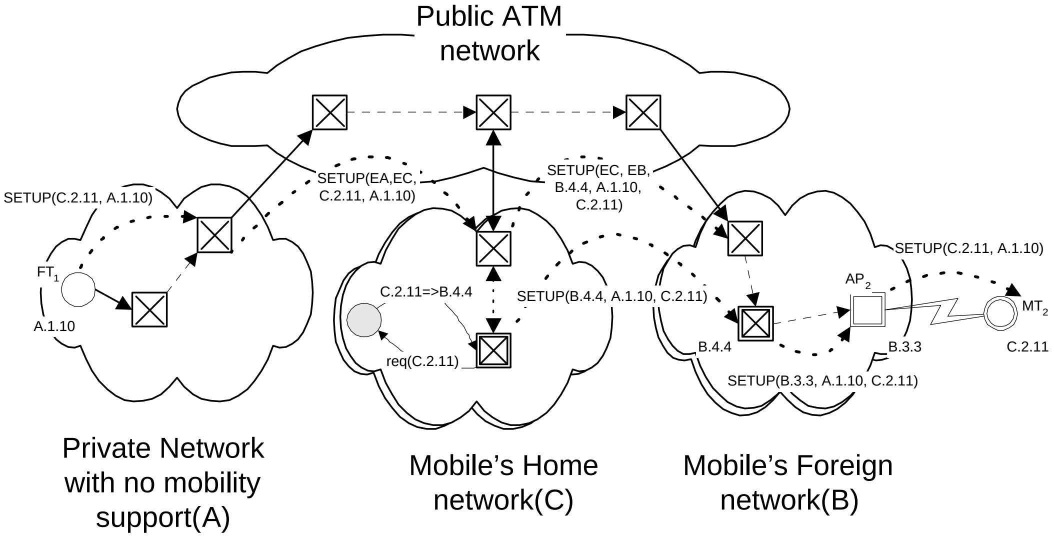
This case is similar to that of a mobile ATM network. In this case the mobile network itself has access points and supports the registration of mobiles. The registration process is hierarchical. Mobile MT_2 registers with the access point AP_2 which itself is part of the mobile network E.

AP_2 registers mobile MT_2 with the Location Service in its own network. This determines the MHA-to-MFA translation specific to the mobile network. The mobile location service then registers MT_2 with the wired location service and the mobile is registered in the usual way in the wired network.

When a connection is made to the mobile there are now two translations of MHA-to-MFA; first by the mobile-enabled switch in the wired network and the second by the mobile-enabled switch (AP_3) in the mobile ATM network.

2.7 Tunnelling through public network

2.7.1 FT to MT via Home Network


Public ATM network
SETUP(C.2.11, A.1.10)
SETUP(EA,EC, C.2.11, A.1.10)
SETUP(EC, EB, B.4.4, A.1.10, C.2.11)
FT1
A.1.10
C.2.11=>B.4.4
req(C.2.11)
SETUP(B.4.4, A.1.10, C.2.11)
SETUP(C.2.11, A.1.10)
AP2
MT2
B.4.4
B.3.3
C.2.11
SETUP(B.3.3, A.1.10, C.2.11)
Private Network with no mobility support(A)
Mobile's Home network(C)
Mobile's Foreign network(B)

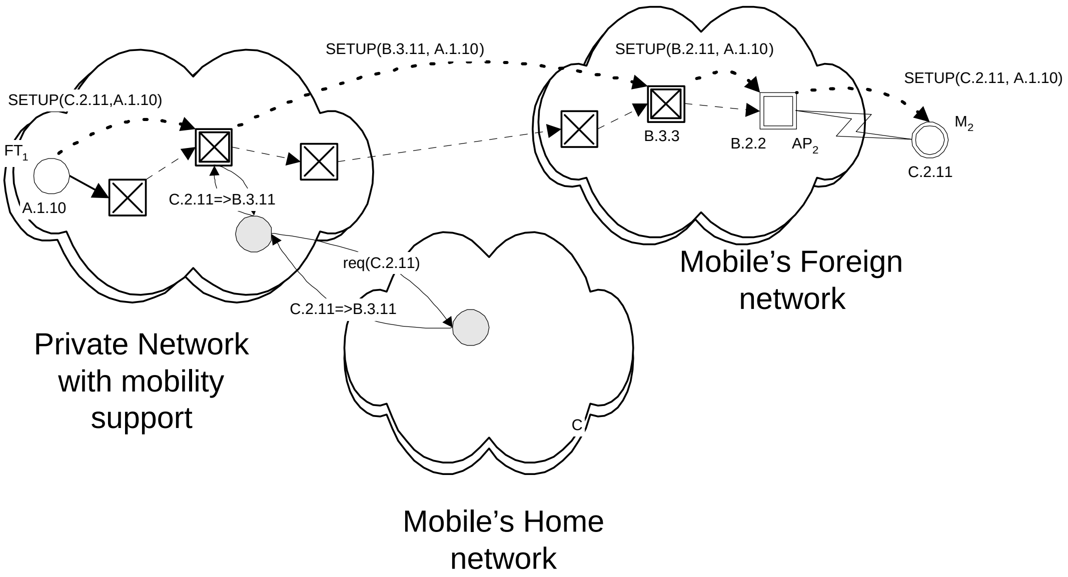
This example demonstrates tunnelling between a fixed host and a mobile endpoint across the public network.
In this case the source network of the fixed host is not mobile-enabled. The mobile is supported by an anchor switch which decouples the movement of the mobile between access points from the Location Service. The protocol falls back to the rerouting approach to location management where the connection is routed via the Home Network of the mobile.

- The call is originated by FT_1 with the MHA as the called party number. There are no mobile-enabled switches in the originating network so the SETUP request is routed to the mobile Home Network by default. The SETUP request traverses the public network using E.164 address encapsulation in order to route to the mobile Home Network.
- In the mobile Home Network the originating NSAP addresses are recovered at the public-to-private UNI and the SETUP request is routed to a mobile-enabled switch.
- This mobile-enabled switch contacts the Location Service (in this case the VLR and HLR may be co-located).
- The MFA B.4.4, the address of the anchor switch, is retrieved from the Location Service.
- The called party number in the SETUP request is replaced with the MFA and the MHA is encapsulated.
- The SETUP request is then routed back through the public network to the anchor switch. In this case the private-to-public UNI must again encapsulate the NSAP addresses using E.164 addresses to identify the appropriate public-to-private network gateway.
- The tunnelled NSAP addresses are recovered at the destination public-to-private UNI and the SETUP request is forwarded to the anchor switch.
- At the anchor switch the tunnelled SETUP request is again recovered and in this case is tunnelled once more to the appropriate access point.
- The access point then forwards the SETUP request containing the original ATM endpoint addresses to the mobile.
- The signalling process completes with either a RELEASE or CONNECT, which follows the reverse path using the prototype VC established by the SETUP request.

In this case the wide area routing is non-optimal due to the lack of mobile support in the source network. The public network is not modified to support mobility and hierarchical tunnelling, i.e. tunnelling for mobility encapsulation and E.164 address encapsulation, is used.

2.8 Implicit Tunnelling

2.8.1 FT to MT



In this example it is assumed that the intervening network cannot support explicit tunnelling. This would be the case for UNI 3.0 / 3.1 networks which have no mechanism for encapsulation of the MHA. Implicit tunnelling requires the MHA and MFA to have a one-to-one mapping. This can be achieved by including the ESI of the MHA in the MFA with the assumption that the mobile ESI is unique.

The MFA is not associated directly with any endpoint in the network. In a SETUP request with the MFA as the called party number, the HO-DSP is used to route the request the appropriate anchor switch. The anchor switch then performs a reverse lookup on the MFA based on the ESI and recovers the appropriate MHA. In this example the SETUP request is again implicitly tunnelled to the access point although it is likely that the anchor switch to access point link will support encapsulation.

3 Summary

The solution described here proposes the use of *tunnelled signalling* in combination with a location service to manage the mobility of ATM devices. The scheme is applicable to both a scenario in which the wireless link is to a mobile terminal and one in which the link is to a mobile. Most importantly it can operate with no changes to signalling protocols and therefore work with existing and future systems.

Advantages of the tunnelling approach:

- Compatible with UNI/PNNI/BICI
- No management load for intermediate switches
- Routing efficient with mobile enabled networks
- Network functional with no mobile enhancements
- Reduces dynamic routing problem in local area
- Can reduce binding overhead especially for mobile networks

Disadvantages:

- Address partition required between mobile and fixed addresses
- Location Service required

4 References

[1] Lou Dellaverson *et al.*, “Proposed Charter, Work Plan and Schedule for a Wireless ATM Working Group”, ATM Forum/96-0721/PLEN, June 10-14, 1996.

[2] A. Acharya, J. Li, and D. Raychaudhuri, “Mapping of contribution 96-1121 (“Primitives for Location Management and Handoff in Mobile ATM Networks”) to WATM baseline text”, ATM Forum/96-1417/WATM, August 1996.

[3] Arun Ayyagari, Jeff Harrang, Sankar Ray, “Call Establishment/Termination in Wireless PNNI”, ATM Forum/96-1410/WATM, October 1996

[4] M. Veeraraghavan, G. Dommety, “Location Management in Wireless ATM Networks”, ATM Forum/96-1500/WATM, October 1996

[5] John Porter *et al.*, “The ORL Radio ATM System, Architecture and Implementation”, Olivetti Research Technical Report 96.5, January, 1996.

[6] The ATM Forum Technical Committee, “ATM User-Network Interface (UNI) Signalling Specification Version 4.0”, af-sig-0061.000, June 1996.

[7] C. Perkins (editor), “IP Mobility Support”, RFC 2002, October 1996.

[8] The ATM Forum Technical Committee, “ATM Name System Specification Version 1.0”, af-saa-0069.000, September 1996.