Internet Engineering Task Force
INTERNET DRAFT

W. T. Teo
S. W. Yeow
R. Singh
National University of Singapore
February 1999

IP Relocation through twice Network Address Translators (RAT)

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document describes a protocol that provides IP reachability for mobile users. Like IP Mobility Support, RFC 2002, each mobile node is accessible by its home address, regardless of its current location in the Internet. When away from home, a mobile node acquires a care-of address indicating its current location. It registers the care-of address with a registration server (RS). The RS sets up a twice network address translation table on a RAT device. The RAT device transparently routes datagrams destined for the mobile node's home address to the care-of address using twice network address translation. The protocol requirements for the mobile node is minimal. End-users can have mobility support easily as registration is done using widely available applications.

1. Introduction

IP version 4 datagram routing generally depends on the destination host's IP address to uniquely identify the host point of attachment in the Internet. This implies a host has to be on the network indicated by its IP address - the home address in Mobile IP (MIP) terminology - to receive packets destined to it.

This document proposes protocol enhancements to network address translators (NAT) which allow other hosts to initiate communication using a mobile node's home address when the latter changes location.

This document does not attempt to describe address translations at a RAT device above the network level. RAT only deals with network address translation of the IP header. Network Address Port Translation (NAPT) and Application Level Gateways (ALGs) can continue to operate on top of RAT.

1.1 IP Reachability Using Twice Network Address Translators

When a mobile node moves from its home network to a foreign network, it acquires a care-of address from the foreign network indicating its current location on the Internet. It will use this topologically correct IP address as its source address when sending out packets. (When the mobile node is at home, the topologically correct IP address will be its home address).

In a foreign network, the mobile node registers the acquired care-of address with a registration server (RS) at home. On successful registration, the RS sets up a twice network address translation entry on a RAT device.

Once setup, the RAT device will transparently route datagrams destined for the mobile node's home address to its registered care-of address by twice NAT [refer to Section 6].

Twice NAT is only required when the mobile node is not at home and the network connections are initiated by the correspondent nodes (CNs), e.g. when the mobile node is an application server. For all other conditions, the mobile node directly communicates with its correspondent nodes, without the overhead incurred from network address translation, i.e. the correspondent nodes respond to the mobile node using the latter's topologically correct address.

1.2 Goals

The main motivation for RAT is to facilitate deployment of IP mobility support. Common network protocols are used to avoid any RAT

specific protocol requirements for the mobile node. effort on the mobile node.

NAT routers are already widely deployed and implementations with twice NAT [REF 3] are available, to provide RAT capability on current NAT [REF 4] devices require minimal enhancements. Networks with NAT installations will be mobile capable by migrating to RAT. By depending on currently available network applications for registration, little effort is needed on the user's part to gain the benefit of mobility.

With network address translations, RAT provides transparent mobility to end hosts. No enhancements to a mobile node's transport and lower network layers are necessary.

The application protocol employed in the registration process is flexible and independent of RAT's base protocol. However, for interoperability reasons, the control messages between a registration server and a RAT device must be followed.

1.3 Applicability

The protocol does not attempt to maintain transport and higher-layer connections when a node changes location. The main function of RAT is to allow correspondent nodes to locate a mobile node by its permanently assigned home address.

1.4 Deployment Issues

In a basic setup, to support RAT, a network needs a registration server and a RAT device for each physically partitioned subnet. The mobile node does not require foreign networks to support RAT to have mobility support. However, the node must be able to acquire a topologically correct IP care-of address via any available external mechanism in the foreign location.

1.5 Protocol Requirements

The mobile node must be able to access at least one of its registration servers when in a foreign location.

The RAT device must be able to deliver datagrams to, and accept datagrams from, the mobile node's foreign location.

All messages used to inform the registration server of the mobile node's current location must be authenticated to protect against remote redirection attacks.

1.6 End Host Accessibility

The correspondent node does not need to know how to reach the RAT device. It sends datagrams to the mobile node's home address, where they are intercepted by the RAT device as necessary.

All correspondent nodes will be able to reach the mobile node if its currently assigned IP address is reachable by the RAT device using the appropriate routable addresses.

Correspondent nodes previously accessible by a mobile node at home may not be reachable when the mobile node is in a foreign location. This is because the correspondent node's access control list or network firewall may deny traffic originating from the mobile node's current location. This is not a design flaw since the existing security policies should not be circumvented for mobility support.

Another reason why a mobile node cannot reach certain correspondent nodes is when the latter are in a network using private IP addresses [REF 2] and the mobile node has moved outside the private network, or when the mobile node has moved into a private network without NAT support. The protocol should not allow a mobile node to reach these correspondent nodes unless the security policies permits.

Private correspondent nodes can still reach a mobile node outside the internal network using RAT. The RAT device may deny the forwarding of such datagrams for security reasons and send an ICMP Host-Unreachable error to the correspondent node.

2. Terminology

This document adopts the terminology (e.g. Care-of address, Correspondent Node, Foreign Network, Home Network) defined in "IP Mobility Support" [REF 1] and "IP Network Address Translator Terminology and Considerations" [REF 3].

In addition, three new entities are introduced :

1. Zero Implementation Mobile Node (0MN)

Zero Implementation Mobile Node (0MN) identifies a mobile host that uses RAT. This is to differentiate the former from the same term used in Mobile IP.

2. Registration Server (RS)

A registration server is generally located in the mobile node's home domain. A 0MN must inform the RS of its new location in a foreign

network before it can receive datagrams destined for its home address. For the registration process to succeed, the RS needs to be reachable from the mobile node's current location using the available routing mechanisms.

The registration server will interact with a RAT device to set up the twice network address translation table (RAT table). Each entry in the table associates a mobile node's home IP address with its care-of address and the binding's lifetime.

The discovery of a registration server is not specified by the protocol and is dependent on the application protocol used in the registration process. For example, if the registration server uses HTTPS for registration, a mobile user may identify the RS by a URL address. In the simplest configuration, the RS address can be statically configured.

3. Twice Network Address Translator for Reachability (RAT device)

The RAT device maintains the association between the home IP address of each 0MN, its care-of address and the binding's lifetime. It uses twice NAT to route datagrams from a 0MN's home address to its care-of address.

The RAT device is generally directly connected to the 0MN's home network in order to receive datagrams destined for the latter e.g. by proxy ARP. The requirement is unnecessary if the RAT device can interoperate with the Mobile IP's home agent entity [REF 1]. The home agent can then tunnel datagrams destined for the 0MN to the RAT device for final delivery to the 0MN's care-of address.

It is not necessary for a 0MN to know the identity of the RAT device for the protocol to work. For security as well as scalability, it is preferred that the RS and the RAT device are on different hosts and only the RS should know the RAT devices available on a network.

3. Registration Application Protocol Selection

The application protocol used by a mobile node to register its current care-of address with a registration server is independent of the protocol. However, For security reasons, the application protocol must fulfill the following criteria :

1. A mechanism to validate both the mobile node/user identity and its current location.

   A registration server must never assume the source IP address of a registration request is the care-of address of the mobile node.

Information disclosure could provide means of hijacking mobile node traffic. Therefore it is recommended that the mobile node's care-of address be encrypted. Using a user-centred authentication scheme, the mobile node's home IP address need not be sent during the registration process if the registration server maintains a mobile user to home address association.

2. A mechanism to confirm that the mobile node is still at its current registered location.

   The mobile node will need to renew its care-of address by re-registration or some similar mechanism, within an appropriate lifetime. This is to avoid forwarding datagrams to an old location the mobile node has vacated. This renewal request should be time-stamped etc to avoid possible replay attacks.

For easy deployment of RAT as a mobility solution, the application protocol used should be widely supported on all operating platforms. A good example of an application protocol that meets the above security and availability requirements is the Secure Hypertext Transfer Protocol (HTTPS), which is HTTP over a Secure Socket Layer (SSL).

A mobile user will only need a World Wide Web (WWW) browser to access a WWW server on the registration server. Java applets may be downloaded from the registration server to request user authentication. With verification of user identity, the applet can then transmit time-stamped "keep alive" beacons back to the RS to confirm the 0MN location. The messages sent can be encrypted/ authenticated using a private key the mobile user provided. The method of encryption/authentication need not be known to any entity except the registration server.

The specifics of the registration process are beyond the scope of this document.

4. Acquiring Care-Of Address

When a 0MN is in a foreign network and desires mobility support, it must acquire a topologically correct IP address in the network. Any available external mechanism supported by the mobile node can be used to acquire a care-of address. Popular protocols available are the Dynamic Host Configuration Protocol (DHCP) or the Point to Point Protocol (PPP).

5. Control Messages

Control messages are used to exchange information between the

registration server and RAT device. It is not recommended that both entities reside on the same machine for the following reasons :

1. The application protocol used for registration may change with the introduction of newer technology but the RAT mechanism will remain the same.

2. Address translation incurs a large overhead in memory and computation [refer to Section 9] and dedicated hardware may be needed. Administration and installation of myriad feasible application protocols on dedicated hardware is not viable.

3. Failure of the registration server or RAT device will deny mobility services. Introducing backup registration servers and alternative RAT devices can increase reliability and distribute load.

The control messages are sent with UDP [5] using the well-known port number 434 allocated to Mobile IP. New authentication extensions are defined to indicate RAT operation. The default authentication algorithm uses keyed-MD5 [6] in "prefix+suffix" mode to compute a 128-bit "message digest" of the control message.

5.1 RAT Translation Binding (RTB) Request

A registration server sends a RAT Translation Binding Request (RTBR) to a RAT device to set up the RAT table - 0MN's home address, care-of address, binding's lifetime.

The Mobile IP registration request format is used.

The format is as follows :

IP fields:

SA: Typically the interface address from which the registration server sends the message.

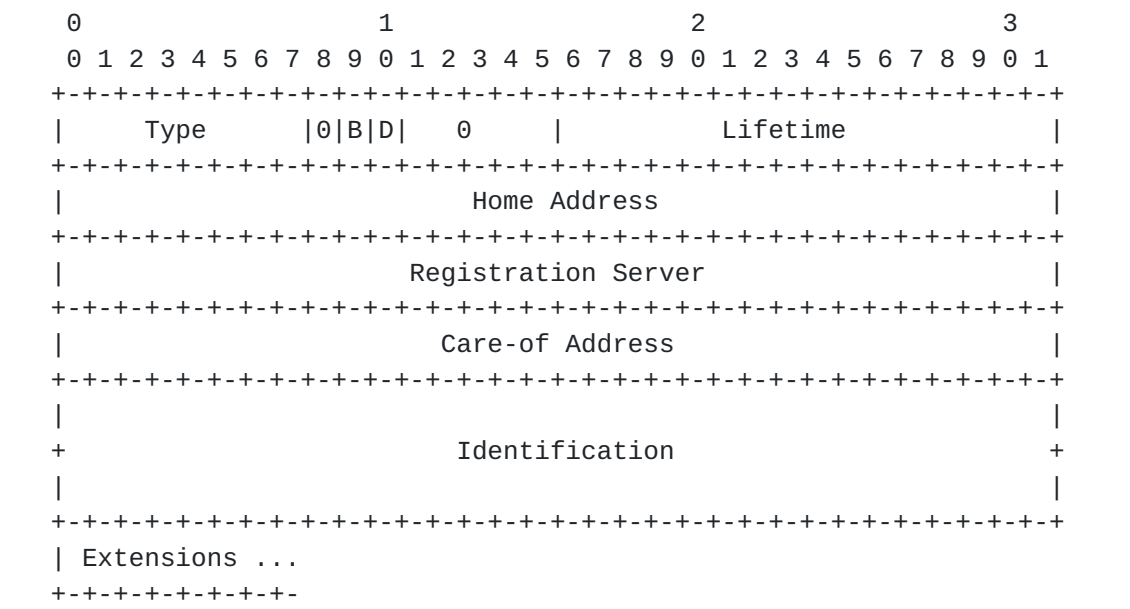
DA: Typically that of the RAT device.

UDP fields:

Source Port: variable

Destination Port: 434

The UDP header is followed by the RAT fields shown below:



Type 1 (Registration Request)

B Broadcast datagrams. If the 'B' bit is set, the registration server requests that the RAT device forwards any broadcast datagrams that the 0MN receives on the home network.

D Decapsulation by RAT device. If the `D` bit is set, the RAT device will decapsulate datagrams which are tunneled from a Mobile IP's home agent [Refer to Section 8].

Lifetime
The number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

Home Address
The IP address of the 0MN.

Registration Server
The IP address of the 0MN's registration server.

Care-of Address
The IP address of the 0MN current location.

Identification
A 64-bit number, constructed by the registration server node, used for matching RTB with RTB Replies, and for

protecting against replay attacks of RTB messages.

Extensions
The fixed portion of the RTB Request is followed by one or more of the Extensions. The RAT-Server Authentication Extension MUST be included in all RTB Requests.

5.2 RAT Translation Unbinding (RTU) Request

When a 0MN is no longer at its registered care-of address, i.e. no "keep alive" beacons are sent by the 0MN to the registration server or its RAT translation binding's lifetime expires, the registration server must send a RAT Translation Unbinding Request to the RAT device to remove the 0MN entry in the RAT translation table.

The format of the RTU request is the same as the RTB request except the lifetime field is 0.

5.3 RAT Control Message Reply

A RAT device returns a Control Reply message to a registration server which has sent a RTB or RTU message.

The Mobile IP registration reply format is used.

The format of the extension is as follows :

IP fields:

SA: Typically copied from the destination address of the RTB or RTU Request to which the RAT device is replying.

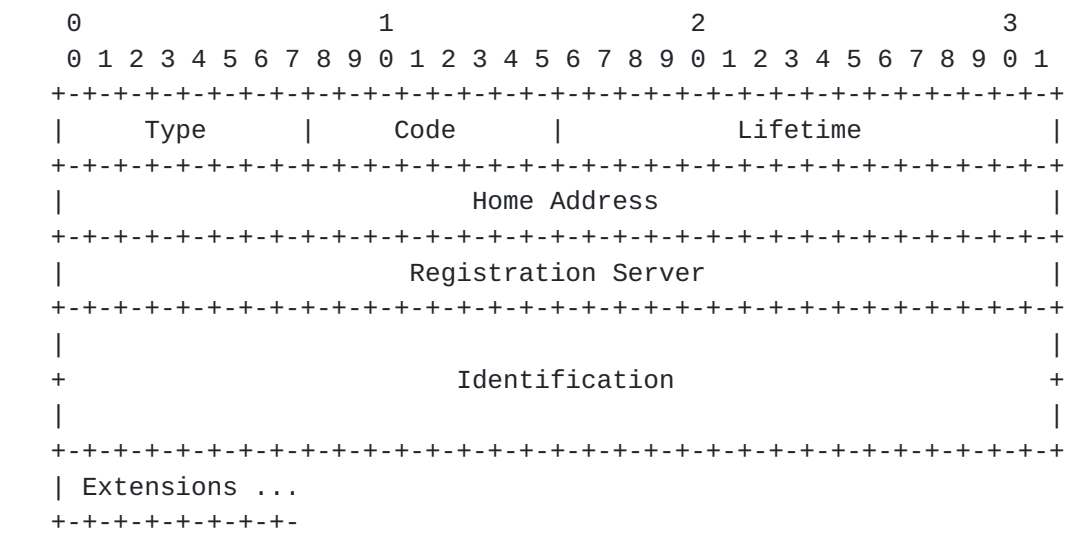
DA: Copied from the source address of the RTB or RTU request to which the agent is replying

UDP fields:

Source Port: <variable>

Destination Port: Copied from the source port of the corresponding RTB or RTU Request

The UDP header is followed by the RAT fields shown below:



Type 3 (Registration Reply)

Code A value indicating the result of the Registration Request. See below for a list of currently defined Code values.

Lifetime
If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and MUST be ignored on reception.

Home Address
The IP address of the 0MN.

Home Agent
The IP address of the 0MN's registration server.

Identification
A 64-bit number used for matching RTB or RTU Requests with RTB or RTU Replies, and for protecting against replay attacks of RTB or RTU messages. The value is based on the Identification field from the RTB pr RTU Request message from the mobile node, and on the style of replay protection used in the security context between the registration server and its RAT device (defined by the security association between them, and SPI value in the Server-RAT Authentication Extension).

Extensions
The fixed portion of the RTB or RTU Reply is followed by one or more of the Extensions. The RAT-Server Authentication Extension MUST be included in all Control Replies returned by the RAT device.

The following values are defined for use within the Code field. RTB or RTU successful:

0 registration accepted

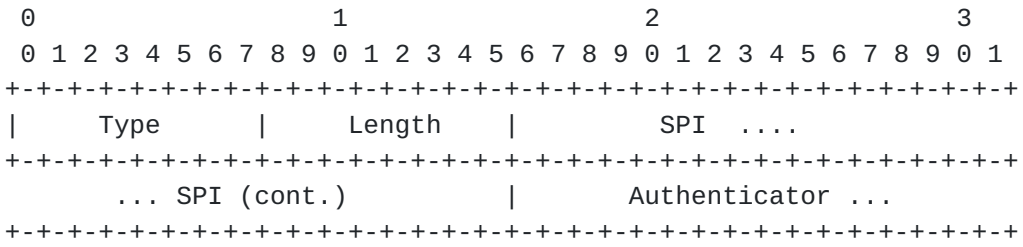
RTB or RTU unsuccessful:

64 reason unspecified
65 administratively prohibited
66 insufficient resources
68 registration server failed authentication
69 requested Lifetime too long
70 poorly formed Request
128 reason unspecified
129 administratively prohibited
130 insufficient resources
133 registration Identification mismatch
134 poorly formed Request
136 unknown registration server address

5.4 RAT-Server Authentication Extension

A RAT-Server Authentication extension type is defined to indicate support for RAT operation.

The format of the extension is as follows :



Type 36

Length 4 plus the number of bytes in the Authenticator.

SPI Security Parameter Index (4 bytes). An opaque identifier.

Authenticator (variable length)

If the extension is missing in a RTB or RTU request and the RAT device is also a Mobile IP home agent entity, it must process the message as a registration request as specified in Mobile IP.

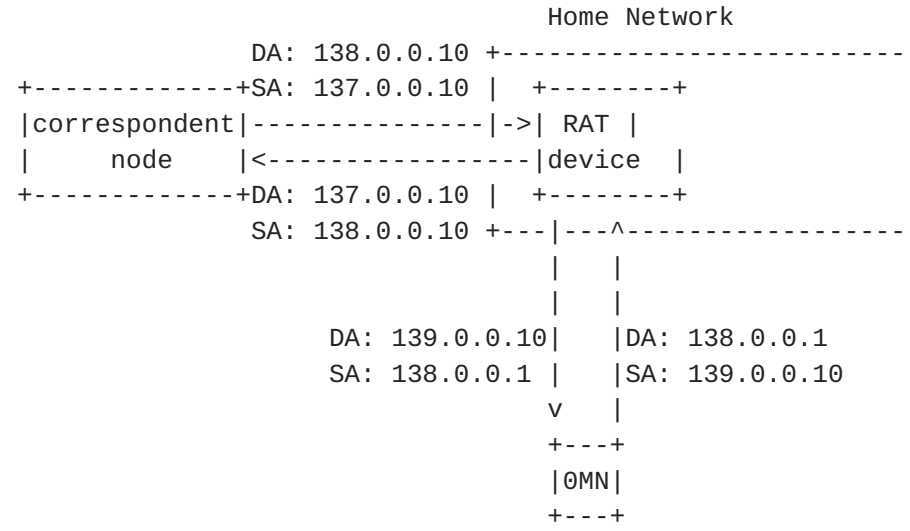
6. Twice Network Address Translation in RAT

On successful registration with a registration server, a 0MN is associated with the tuple <home address IP, care-of address IP>. For any session initiated by a correspondent node, all requests and reponses must be routed via the same RAT device.

Any datagram with a destination address that is a registered 0MN's home address in the RAT table must be reverse address translated. Any reply from the registered 0MN to the RAT device must be similarly translated.

The following example illustrates the operation of a RAT device at the network level. Network Address Port Translations and Application Layer Gateways' operations (if any) are not illustrated.

```
Correspondent Node Address:   137.0.0.10
Home Network:                 138.0.0.0/24
0MN home address:             138.0.0.10
0MN care-of address:          139.0.0.10
RAT device address:           138.0.0.1
```



7. ICMP Error Translation

When a RAT device receives an ICMP Destination-Unreachable error message for datagrams destined to a care-of address in the RAT table,

the error message should be translated as follows :

IP fields:

SA: RAT device's outgoing interface address to correspond node
DA: correspondent node address that initiated the session

ICMP field:

Type: 3

If the ICMP code indicates network unreachable, it should be replaced by the corresponding host unreachable number. The IP header embedded within the ICMP payload must be similarly modified.

8. Comparisons

8.1 NAT and RAT comparison

Network Address Translation (NAT) is typically used when a network's internal IP addresses cannot be used externally. NAT can connect separate routing realms with different addressing schemes. It does that by translating the network address of datagrams to the appropriate routable address in the corresponding routing space. Therefore NAT is used when the end hosts are in different routing realms. The NAT device must be assigned an address in each of the routing realms it connects.

The purpose of RAT is different. RAT is used even when the end hosts are in the same routing space to forward datagrams destined to the mobile node's home address to the latter's care-of address. The RAT device only needs to be assigned one address if all end hosts are in the same routing space.

RAT does twice Network Address Translation [REF 3] for datagram delivery. In twice NAT, both the source and destination addresses are translated. The current reason for twice NAT is to connect end hosts that use overlapping address space in their home network. A unique intermediate address space is used to connect the end hosts i.e. the RAT device becomes the virtual sender/receiver of the mobile/correspondent nodes.

NAT is always needed for communicating hosts in separate routing realms regardless of the session direction [REF 3]. RAT is needed only when the session is intiated by the correspondent nodes. In traditional NAT [REF 4], translation is initiated by the client nodes which the NAT device services. RAT translation is initiated in reverse by the correspondent nodes and by not the mobile client nodes

which the RAT device services.

8.2 Mobile IP and RAT comparison

The Network Address Translator (NAT) and NAPT have become popular because of easy deployment. They require no modifications to the communicating hosts. Mobile IP however faces difficulties in deployment as all mobile nodes need to support the protocol. While implementation and deployment of Mobile IP home agents need not be concerned with the operating system, mobile users are constrained to operating systems which supports Mobile IP. Network adminstration for Mobile IP's security authentication and key allocation also requires additional configuration tools for the novice user.

The base protocol of Mobile IP does not support communication across different routing realms e.g. between private and public nodes. If such mobility support is desired, Mobile IP extension for Private Internets Support [8] or Firewall Support for Mobile IP [9] is needed. NAT's main function is to allow communication between different routing realms. If the current NAT installation already support such communication for sessions initiated in any routing realm, RAT can provide the mobility support without additional enhancements.

Mobile IP uses IP tunneling to deliver datagrams to a mobile node's care-of address. This allows a mobile node to bypass traditional firewalls that only filter packets based on the IP tunnel header. RAT uses twice NAT/NAPT to deliver datagrams to a mobile node's care-of address. Certain applications which embed the end hosts' IP addresses in the data payload will not function with NAT/NAPT if there are no application layer gateways available to support them.

Mobile IP specifies the registration message formats and semantics for mobile nodes. RAT uses common application protocols supported on any network operating systems. The delivery mechanism - twice NAT/NAPT - is explicitly separated from the registration mechanism in RAT.

RAT provides limited mobility in comparison to Mobile IP. It does not attempt to maintain connection orientated sessions while the mobile node moves across multiple networks.

Where the abovementioned limited mobility and application support is sufficient, RAT is much easier as a deployment solution.

In Mobile IP, there are 2 main purposes for a mobile node to have a fixed IP address - the home IP address :

1. To enable all correspondent nodes to identify the mobile node with a fixed IP address that is unchanged regardless of location.

2. To retain connection orientated transport protocols, e.g. TCP connections, while the mobile node moves across networks.

The intended function of RAT is to achieve the first purpose. It is typically unnecessary for the mobile node in a foreign location to use its home IP address as the source IP address when originating a datagram.

Such an approach as defined in MobileIP has two disadvantages :

1. Datagrams originating from the correspondent node will generally need to be routed to the mobile node's home network before they are tunnelled to the mobile node care-of address.

2. If Ingress filtering is deployed at the mobile node's current foreign location to filter datagrams with topologically incorrect source IP address, bidirectional tunneling is required to bypass the Ingress filter.

Both of the above situations may result in a longer routing path between the sender and receiver.

In RAT, for a correspondent node initiated session, the end hosts' routing path is similiar to bidirectional tunneling in Mobile IP. This will form a dog-legged route, from the mobile node to RAT device to correspondent node and vice versa.

For communication initiated by the mobile node, since both the end hosts' addresses used are topologically correct, standard IP routing is sufficient and RAT is not be involved. However, communication will fail in situations where the home IP address is necessary e.g. where IP datagrams originating from the care-of address of a 0MN are blocked by a firewall, but not those originating from its home address.

Interoperation with Mobile IP

The basic RAT protocol is meant to provide a fast and simple mobility solution. Its main advantage is any node can be mobile if desired as no RAT-specific protocol support is needed for a 0MN. To push forward the deployment of a Mobile IP infrastruture, RAT is designed so that it can be incrementally enhanced to support a gradual installation of Mobile IP entities. This is possible mainly because RAT adopts the same format and semantics of Mobile IP registration messages. The following section describes how mobility support can

migrate from RAT to Mobile IP.

For the initial adoption of Mobile IP, home agents are deploy instead of RAT devices at every network segment. Since the home agents' operating platform and hardware do not affect the mobile user, any available home agent implementation can be selected. The end result is that, instead of one RAT device for every network segment, a home agent can intercept the 0MNs' traffic on behalf of the RAT device i.e. the RAT device is no longer bound to one home network segment.

1. Migration Step 1

To interoperate with home agents, the RAT device will need to add support for IP tunnel decapsulation. After accepting a registration request from a 0MN, the registration server will now additionally send a Mobile IP registration request to the home agent on behalf of the 0MN, with the RAT device specified as the tunnel endpoint. Mobile traffic delivery is now tunneled from the home agent to the RAT device and the RAT device will do address translation to deliver the traffic to the 0MN.

2. Migration Step 2

The next transition phase is to support IP decapsulation at the mobile node. The movement detection and registration process remain unchanged, but mobile traffic delivery will no longer require a RAT device. The registration server will send Mobile IP registration requests to the home agents as Step 1 but now the tunnel endpoint is not the RAT device but a mobile node. In this model, seamless mobility is now achievable.

3. Migration Step 3

The final step to full Mobile IP support will require the mobile node to support movement detection and perform registration as specified in Mobile IP. In this stage, the registration server is no longer required; however the benefits of a central entity for managing mobility policies may argue for retaining the registration server. In such a configuration, the registration server acts as a trusted registration proxy between the mobile node and its home agent. Mobile nodes need only know its registration server address. All home address to home agent address associations are maintained at the registration server, allowing transparent handover to alternative home agents in the event of a home agent failure or migration.

For details on RAT to Mobile IP migration, see [REF 10].

10. Scalability Issues

The overhead of maintaining address tables and performing address translations is computationally intensive. This implies the RAT device is a possible bottleneck and point of failure. If there are alternative RAT devices, recovery of the RAT table during a RAT device failure is possible with the information stored in the registration server.

Furthermore, the RAT device must be able to determine the CNs and 0MNs association for each IP datagram that it receives, in order to perform address translation.

Address translation can be performed at two levels, and both require the RAT device to possess a pool of IP addresses. The scalability limitations of the protocol depend on which method is employed.

10.1 RAT with only Twice Network Address Translation

The RAT device examines the source and destination IP addresses of each packet to determine the CN and 0MN association. This is simply referred as RAT in the previous sections.

To eliminate ambiguity, the RAT device must associate a unique IP address from its pool of addresses for each CN that is currently communicating with a 0MN. This IP address is used by the RAT device to determine the end hosts' IP for datagrams between the RAT device and registered 0MNs. The number of CNs that are able to connect to 0MNs during any period of time is thus limited by the size of the RAT device's IP address pool.

This approach has the advantage of being independent of the protocols above the network layer.

10.2 RAT with Twice Network Address and Port Translation

The RAT device maps an IP datagram to its associated CN and 0MN by using three additional fields: the IP protocol type number and the transport layer source and destination connection identifiers (e.g. TCP port number or ICMP echo request/reply ID field). This is labeled as IP Reachability Using Twice Network Address and Port Translation (RAPT).

RAPT does not have the same limitations on scalability as RAT, since the limit on the number of concurrent connections possible between CNs and 0MNs is much larger in RAPT than in RAT.

However, RAPT scalability is limited by its inability to support protocols that do not employ a transport layer connection identifier.

11. RAT Limitations

For any sessions that requires RAT when a mobile node is not at home, applications or security mechanisms that fail with NAT/NAPT with no available specific application layer gateway (ALG), will similarly fail with RAT.

RAT is subjected to additional limitations listed in [REF 1] when address translations are necessary.

12. Current Implementation

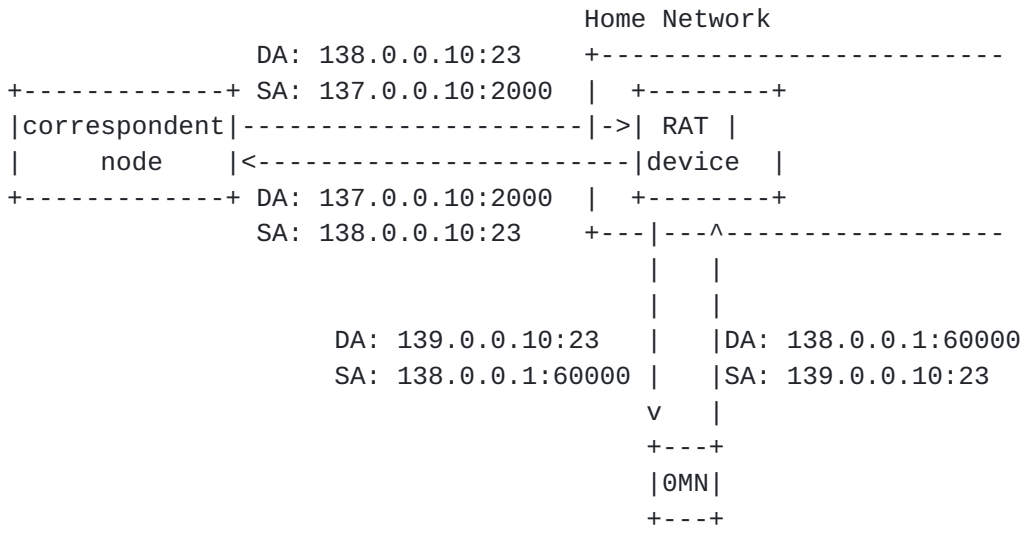
A prototype implementation of RAT based on NAPT is now under development at http://cram.comp.nus.edu.sg:8080/cram/rat/. It supports TCP, UDP and ICMP. Application-level gateways are required for most protocols layered on top of these, including FTP, RTSP and HTTP.

To differentiate CN-to-0MN from 0MN-to-CN datagrams, the source and destination IP addresses, port numbers and transport protocol of each IP datagram received at the RAT device are examined. The datagrams are then translated as illustrated in the following diagram before being forwarded by the RAT device:

Translation of CN-to-0MN and 0MN-to-CN IP datagrams:

```
 Correspondent Node Address:   137.0.0.10
 Home Network:                 138.0.0.0/24
 0MN home address:             138.0.0.10

 0MN care-of address:          139.0.0.10
 RAT device address:           138.0.0.1
```



13. Security Considerations

The security considerations described in [REF 1] for all variations of NATs are applicable to RAT when address translations are necessary.

A security log must be maintained at the registration server. Each registration request <home IP address, care-of address, time> should be recorded.

If simultaneous valid registration requests with different care-of addresses from the same mobile node is received, the event MUST be logged. The registration server must discard all future registration requests from the same mobile node. A registration failure message should be sent to the requested care-of address if the application protocol supports error handling. The format of the message will be dependent on the application protocol used.

All registration failures MUST be logged. The mobile user should be informed the time of the most recent successful/failed registration for each new registration attempt if possible.

Acknowledgements

Many thanks to Dr Y. C. Tay, National University of Singapore, and P. Srisuresh, Lucent Technologies, for their valuable help in reviewing this document.

RAT research and development is funded in part by the National University of Singapore ARF grant RP960683.

References

[1] Perkins, C., Editor, "IP Mobility Support", RFC 2002, October 1996

[2] Rekhter, Y., Moskowitz, B. Karrenberg, D., G. de Groot, and Lear, E. "Address Allocation for Private Internets", RFC 1918, February 1996

[3] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", <draft-ietf-nat-terminology-01.txt> - work in progress, October 1998

[4] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", <draft-ietf-nat-traditional-01.txt> - work in progress, November

1998

[5] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980

[6] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992

[7] Perkins, C., "IP Encapsulation within IP", RFC 2003, May 1996

[8] W. T. Teo, Y. Li, "Mobile IP extension for Private Internets Support", <draft-teoyli-mobileip-mvpn-01.txt> - work in progress, November 1998

[9] Montenegro, G., Gupta, V., "Sun's SKIP Firewall Traversal for Mobile IP", RFC 2356, June 1998

[10] R. Singh, Y. C. Tay, W. T. Teo, S. W. Yeow, "RAT: A Quick (And Dirty?) Push for Mobility Support", Proceedings of IEEE Workshop on Mobile Computing Systems and Application, February 1999 http://cram.comp.nus.edu.sg:8080/cram/rat/

Author's Address

W. T. Teo
National University of Singapore
School of Computing
Lower Kent Ridge Cresent
Singapore 119260

EMail: teoweetu@comp.nus.edu.sg

S. W. Yeow
National University of Singapore
School of Computing
Lower Kent Ridge Cresent
Singapore 119260

EMail: yeowshin@comp.nus.edu.sg

R. Singh
National University of Singapore
School of Computing
Lower Kent Ridge Cresent
Singapore 119260

EMail: rhandeev@comp.nus.edu.sg